Computer Networks

Fragenkatalog S23

Organisatorisches

Zoom-Link:
https://tuwien.zoom.us/j/61469610859?pwd=RExtNFNQMU5BL1dyd2hFUUdpT2Y2dz09

Bsp.: Computer Networks SS21 Computer_Networks_Master_S2021.pdf
Bsp.: Computer Networks SS22 Computer Networks Collaborative Mitschrift

Gruppenarbeit

- Gruppenarbeit für je drei (eventuell vier) Personen zum Thema “Stabilität”
- genaue Themenwahl innerhalb von drei Wochen ab der Vorbesprechung
- Vortrag muss *genau* 15 Min. dauern, sonst wird abgebrochen
    - 1. Vortrag soll genau 10 Min. dauern
- Folien sind nicht notwendig
- beim Vortrag am Ende sollten alle zum Reden kommen

- erster Vortrag nach Ostern
- max 10 Minuten
- was haben wir vor zu tun und welche Stolpersteine erwarten wir. Welche Ergebnisse erwarten wir
- nicht beurteilt
- **Finale Präsentation ist irgendwann in den 2 Wochen nach der Prüfung**
- **Paper Abgabe: 10.07.2023**

Prüfung

- **mündlich**
- aus Fragenkatalog, nachfragen nach Hintergrundwissen ist möglich

Vortrag (bzw. 1. Vortrag)

Wie soll ein Vortrag ausschauen?

- Begrüßung
- Vorstellung (Name, etwas zur eigenen Person, evtl. Spezialität)
- Einleitung (ca. wie Abstract)
- Inhaltsangabe (Welche Punkte werden behandelt?)
    - Motivation
    - Was wollen/werden wir machen?
- Inhalt
- Ende

        - abrupt (offen, eher vermeiden)
        - abrunden (besser)
        - Möglichkeit der Rückfrage muss gegeben sein (z.B. Aufforderung ans Auditorium)

Generell:

- Füllwörter vermeiden (ist ihm sehr wichtig)
- strategische Pausen (Spannungsaufbau)
- Folien optional
- Wie soll eine Folie aufgebaut sein?
    - Kontrast so, dass Schrift auch von letzter Reihe erkennbar ist
    - Viel Text = Todessünde (nicht machen)
    - Folien sollen Hilfsmittel sein für die Vortragenden, nicht umgekehrt
- Nicht auf die Folie/Tafel schauen -> sondern ins Auditorium reinschauen
- Laserpointer vermeiden, eher mit Maus etwas auf den Folien zeigen
- Gestik: gut, aber nicht zu viel bewegen
- Sprache
    - deutlich, laut

Feedback

- Inhaltlich
- Art der Präsentation

Organisatorisches
    Gruppenarbeit
    Prüfung
Gestellten Fragen:
    VO1 - 01.03.2023:
    VO2 - 08.03.2023:
    VO3 - 15.03.2023
    VO4 - 22.03.2023
    VO5 - 29.03.2023
    VO6 - 03.05.2023
    VO7 - 10.05.2023
    VO8 - 17.05.2023
    VO9 - 31.05.2023
Fragen ausgearbeitet:
    VO2
    VO3
    VO4
    VO5
    VO6
    VO8
    VO9
    VO10

Vorlesungen:

- VO2
- VO3
- VO4
- VO5
- VO6
- VO7
- VO8
- VO9
- VO10

Gestellten Fragen:

VO1 - 01.03.2023:

- Vorbesprechung!

VO2 - 08.03.2023:

- Was ist der Unterschied zwischen Verstärkung und Regeneration?
    - Beim Verstärken werden alle Störungen verstärkt, beim Regenerieren wird das Signal (so wie es möglicherweise fehlerhaft empfangen wurde) sauber reproduziert.
- Was wird benötigt, damit die Kommunikation in Shared Media funktioniert? (Voraussetzungen)
    - Zugriffssteuerung: Es muss ein Mechanismus vorhanden sein, der bestimmt, welcher Host zu welchem Zeitpunkt das Medium nutzen kann. (Kollisionen)
    - Adressierung
    - Fehlererkennung?
- Was ist der Unterschied zwischen Uni, Multi- und Broadcast? (Nachfrage: Welchen Vorteil und welchen Nachteil hat Broadcast?)
    - Broadcast ist eine Belastung für alle (ganzes Netzwerk)
    - Broadcast kann ein Netzwerk lahmlegen, frisst Bandbreite
- Wie entwickelt sich der Signal-to-Noise Ratio (SNR) mit zunehmendem Übertragungsweg?
    - Einheit Dezibel: Verhältnis, wenn negativ: dämpfung, wenn positiv: verstärkung
    - Formel: $10 \times log(\frac{a}{b})$
        - https://de.wikipedia.org/wiki/Leistungspegel
    - 0 Dezibel: referenz Stärke
    - SNR von 0 Db: Signal und Noise ist gleich stark
    - th. -20db nicht mehr hörbar
    - Glasfaser Dämpfungsbudget: 7db
- Was passiert mit einer elektromagnetischen Welle, wenn sie an einer Störstelle trifft?
    - Welche Form hat eine Welle? Sinus
    - Was macht man, wenn man keine Sinus-Form haben mag? Fourier-Transformation
    - Summe von Sinus-Kurven zur Annäherung jeglicher Kurvenform
    - Energie hin, kommt zurück - muss verarbeitet werden
    - Teil reflektiert, Teil transmittiert
    - Grenzschicht (bspw Luft auf Glas)
    - Grenzschicht nicht exakt -> Streuung
    - Absorption (bspw Glas wird heiß)
    - 3 Effekte:
        - Reflexion

        - Absorption
        - Transmission
        - (Absorption - Stehende Welle, passiert bei Antennen)
            - Variante: Wegzeit von direkter und reflektierter Welle sorgen für Auslöschung (addition beider Wellen)
            - Relevant für WLAN Ausbreitung, nicht in … geführten Leitungen
            - Terminierung der Leitung löst Problem (mit Widerständen)
- Was sind die Vor und Nachteile von Fehlererkennung und Fehlerkorrektur
    - Leitungsgeführt (Glasfaserkabel, Kupferkabel vs Funk (Radio, Antenne)
    - Funk: unbekannte Reichweite

VO3 - 15.03.2023

- Was ist die Schlagzahl bei verdrehten Kabeln?
- Worin besteht das Problem bei Alien Xross Talk?
- Was versteht man unter Xross Talk? (3 Arten)
- Was ist die Fourier-Analyse und wozu braucht man das?
- Unterschiedliche Reichweiten von Richtungsantenne und Stabantenne/Rundstrahlantenne
- Welche Arten von Antennen gibt es und welche Vorteile haben sie?

VO4 - 22.03.2023

- Was beschreibt die EN50173 Norm?
- Was sind Phased-Array Antennen?
- Unterschiedliche Qualitätsbezeichnungen Klasse vs. Kategorie
- Was sind Vorteile und Nachteile von PoE (Power over Ethernet)?
- Unterschied zwischen Permanent Link und Channel
- Kabelmengen: z.B. Favoritenstraße, Grundfläche, Arbeitsplätze, Etagen, Kabel pro Arbeitsplatz … hochrechnen/abschätzen. Auf ~50km genau(falls möglich)
- Unterschied zwischen Pass, Pass* und Fail

VO5 - 29.03.2023

- Mac Table Flooding
- Unterschied Singlemode/Multimode Lichtwellenleiter
- Umgang mit LWL, physikalische Zusammenhänge, biegen, nicht reinschauen etc.
- LWL Verbindungen
- Entfernungen bei (unterschied Multimode, Singlemode)
- CSMA/CD Funktionsweise
- Was ist eine Präambel? (Phasenangleich)
-

VO6 - 03.05.2023

- Wie kann eine Switch-Topologie ausschauen?
- Beschreiben sie den Spanning-Tree Algorithmus
- Zeitverhalten beim Weitersenden eines Pakets durch einen Switch
- Was ist Flapping?
- Was ist link/port aggregation
- Welche Arten von Wachstum gibt es? (horizontal/vertikal)

VO7 - 10.05.2023

- ??? (Weiß hier jemand was?) (Ich glaub nach den Präsentationen hat er nicht nach Fragen gefragt.)

VO8 - 17.05.2023

- Funktionsweise VLAN-Switch
- Was bedeutet “virtuell”?
- Was ist Frequency Hopping?
- VLAN Port-Assignment (3 Möglichkeiten)
- 802.1X Was/Wie/Warum? Authentifizierungsmöglichkeiten bei VLAN
- Was ist ein Trunk?
- Spanning Tree Verhalten bei Störungen

VO9 - 31.05.2023

- Welche IP-Netzklassen gibt es? (class A,B,C, Zusatzfrage: direkt auf Bitebene ablesbar)
- Warum reichen MAC-Adressen für das Internet nicht aus?
- Wozu dienen RFC Adressen? (private, nicht geroutete Adressen)
- Was versteht man unter Maskarading? (Unterschied PAT / NAT)
- IP-Adressberechnung (wichtig siehe VO)
- keine 6. Frage

VO10 - 01.06.2023

- Was ist ARP-Spoofing? (In welchem Bereich kann das auftreten, was kann man dagegen tun?)
- Wozu wird ARP verwendet und was ist das?
- Skizzieren Sie den Aufruf von www.orf.at (DNS-Abfragen als Client, Pakete …)
- Was ist ein Reverse Name Server?
- Was ist ein Name-Server? (Wie hängen Reverse Name-Server und Name-Server zusammen?)
- Was ist DHCP? (Wie kann man es umgehen, welchen Aufwand hat man damit?)

VO11 - 14.06.2023

- Welche Phasen gibt es bei TCP/UDP? (Timeouts, welche Größenordnung von Timeouts)
- Einsatzszenarien für TCP/UDP
- Funktion des 3-Way Handshakes
- Socket - Aufbau/Anwendung
- SYN-Flood-Attacke
- Standard-Ports (Welchen Port würden Sie verwenden bei Ihrer neuen Applikation?)

Fragen ausgearbeitet:

VO2

- **Was ist der Unterschied zwischen Verstärkung und Regeneration?**
  Beim Verstärken werden alle Störungen verstärkt, beim Regenerieren wird das Signal (so wie es möglicherweise fehlerhaft empfangen wurde) sauber reproduziert.

  Wenn ein digitales Signal einige Zeit unterwegs ist, läuft das Signal auseinander (inkohärent). Um das Signal über weitere Strecken zu übertragen gibt es zwei Möglichkeiten: Verstärker und Regenerator/Repeater
  Verstärker vergrößert die Amplitude der Welle ohne die Verzerrung der Wellenform zu korrigieren. Problem: Es wird auch das Rauschen verstärkt.
  SNR wird schlechter.
  Vorteil: Da nur verstärkt wird, ist ein Fehler bei den Bits sehr unwahrscheinlich.

  Regenerator: versucht das ursprüngliche Signal/Timing wiederherzustellen und entfernt Rauschen und Verzerrungen der Pulsform.
  Vorgehensweise: Detektieren, auf höhere Ebene Bitmuster erkennen und dann ein neues Signal erzeugen.

  Probleme:
  - Fehler beim Erkennen
  - Fehler in der Software
  - Fehler beim Generieren

- **Was wird benötigt, damit die Kommunikation in Shared Media funktioniert? (Voraussetzungen)**
  - **genügend Bandbreite:** Funktioniert nur, wenn die benötigte Bandbreite aller Endpoints zusammen weniger ist als die gesamte vom Medium zur Verfügung stehende Bandbreite.
  - **Eindeutiger Namensraum:** Kann sich auf Teilnehmer oder Nachrichten beziehen.
    - CAN-Bus: Nachrichtenbezogen:
      Bei CAN-Bus enthält jede Nachricht eine CAN-ID. Jeder Teilnehmer beim

shared media über CAN-Bus liest alle Nachrichten und entscheidet dann mit der CAN-ID, ob die Nachricht für ihn relevant ist.
        - LAN: Teilnehmerbezogen.
          Adressierung durch eine eindeutige Kennung z.B. IP-Adresse. Diese kann von der Anzahl an Teilnehmern abweichen.
    - **Selbstbeschränkung**: Es sind “Sendepausen” (Inter-Packet Gap) notwendig. Im Zuge dessen auch eine Collision Detection: Wenn mehrere Geräte gleichzeitig Daten senden -> Kollision. z.B. CSMA: stellt sicher, dass ein Gerät vor dem Senden prüft, ob das Medium frei ist. Falls nicht, wartet es eine zufällige Zeitspanne, nach der es wieder prüft.
    - **Zugriffsmethode**: Wer kommt als nächstes dran bei shared media? z.B. CSMA/CD: Kollisionen werden erkannt und Kollisionsbehandlung wird durchgeführt. Oder z.B. Token-Ring.

- **Was ist der Unterschied zwischen Uni-, Multi- und Broadcast? (Nachfrage: Welchen Vorteil und welchen Nachteil hat Broadcast?)**
    - Unicast: Verbindung zu genau einem anderen Host (Punkt zu Punkt Kommunikation)
    - Multicast: Verbindung zu definierter Gruppe an Hosts
      Multicast ist effizienter als Unicast, da die Nachricht nur einmal über das Netzwerk übertragen wird, unabhängig von der Anzahl der Empfänger in der Gruppe. Empfänger müssen richtig konfiguriert sein, um bestimmten Multicast zu empfangen.
    - Broadcast: Verbindung zu allen anderen Hosts im Netzwerk
      Broadcast eignet sich für die Übertragung von Informationen, die für alle Geräte im Netzwerk relevant sind, wie beispielsweise Konfigurations- oder Alarmmeldungen.

  Vor/Nachteile von Broadcast:
    - Vorteile:
        - Einfachheit: Broadcast erfordert keine spezifische Adressierung jedes einzelnen Empfängers. Die Nachricht wird an alle Geräte im Netzwerk gesendet, ohne dass die Quelle die Empfänger explizit kennen muss.
        - Effizienz bei bestimmten Szenarien: Broadcast ist effizient, wenn Informationen an alle Geräte im Netzwerk übertragen werden müssen, z. B. für wichtige Ankündigungen oder Netzwerkwartung.

    - Nachteile:
        - Netzwerküberlastung: Da Broadcast-Nachrichten an alle Geräte im Netzwerk gesendet werden, kann dies zu einer erhöhten Netzwerklast führen. Je größer das Netzwerk ist, desto größer ist das Potenzial für Bandbreitenengpässe und Leistungseinbußen.
        - Sicherheits- und Datenschutzprobleme: Da Broadcast-Nachrichten von allen Geräten empfangen werden, kann es schwierig sein, vertrauliche Informationen zu schützen, da potenziell unbefugte Geräte Zugriff auf die Nachricht haben.

- **Wie entwickelt sich die Signal-to-Noise Ratio (SNR) mit zunehmendem Übertragungsweg?**
  Mit zunehmendem Übertragungsweg nimmt die Stärke des Signals ab, während das Rauschen immer vorhanden bleibt, das Verhältnis daraus nimmt ab.

  Definition SNR:
  Verhältnis der mittleren Signalleistung P_Signal zur mittleren Rauschleistung P_Rauschen

$$\mathrm{SNR} = \frac{\text{Nutzsignalleistung}}{\text{Rauschleistung}} = \frac{P_{\text{Signal}}}{P_{\text{Rauschen}}}$$

  - Einheit Dezibel: Verhältnis, wenn negativ: Dämpfung, wenn positiv: Verstärkung
  - Formel um SNR in dB anzugeben: $10 \times log_{10}(\frac{P_{Signal}}{P_{Rauschen}})$
    - https://de.wikipedia.org/wiki/Leistungspegel
  - 0 Dezibel: referenz Stärke
  - SNR von 0 dB: Signal und Noise ist gleich stark
  - th. -20db nicht mehr hörbar
  - Glasfaser Dämpfungsbudget: 7dB
  - SNR Gegenmaßnahmen:
    - Signalverstärkung, Fehlerkorrekturcodes, dennoch NICHT möglich, vollständig zu verhindern, dass SNR mit zunehmender Entfernung abnimmt.

- **Was passiert mit einer elektromagnetischen Welle, wenn sie auf eine Störstelle trifft?**
  - Absorption:
    - Die elektromagnetische Welle wird vollständig vom Hindernis absorbiert. Die Menge der Absorption hängt von verschiedenen Faktoren ab(Frequenz, Eigenschaften der Störstelle). Die Energie der Welle wird in Wärme oder andere Formen umgewandelt. Es findet keine weitere Ausbreitung statt.
  - Transmission:
    - Die elektromagnetische Welle durchdringt das Hindernis und setzt ihre Ausbreitung auf der anderen Seite fort. Die Intensität der Welle kann jedoch aufgrund von Absorption oder Streuung während der Transmission abnehmen.
  - Reflexion:
    - Die elektromagnetische Welle prallt vom Hindernis ab und ändert ihre Richtung. Der Einfallswinkel ist gleich dem Reflexionswinkel. Die Intensität der reflektierten Welle hängt von der Intensität der einfallenden Welle und von den Materialeigenschaften des Hindernisses ab.
  - Brechung:

        - Die elektromagnetische Welle tritt durch das Hindernis, ändert jedoch ihre Richtung aufgrund einer Änderung der Ausbreitungsgeschwindigkeit. Dies tritt auf, wenn die Welle von einem Medium mit einer bestimmten Dichte in ein anderes Medium mit einer anderen Dichte übergeht. Der Brechungswinkel hängt vom Einfallswinkel und den Materialien ab (den Brechungsindizes der beiden Medien ab und folgt dem Snellius'schen Brechungsgesetz).

- **Was sind die Vor- und Nachteile von Fehlererkennung und Fehlerkorrektur**
  <u>Vorteile:</u>
  - Fehlervermeidung und erhöhte Zuverlässigkeit durch Korrektur bzw. Neuanforderung von Datenpaketen.

  <u>Nachteile:</u>
  - Latenz: Fehlererkennung/Korrektur benötigt Zeit, da die Daten analysiert und korrigiert werden müssen (mögl. Problem bei Echtzeitanwendungen)
  - Overhead: F. Erkennung/Korrektur benötigt Redundanz, es werden also mehr Daten übertragen
  - Komplexität: zusätzliche Rechenleistung und Ressourcen. Dies kann zu höheren Kosten und längeren Verarbeitungszeiten führen.

VO3

- **Was ist die Schlagzahl bei verdrehten Kabeln?**
  - Die Schlagzahl (auch als "Pitch" oder "Twist-Rate" bezeichnet) bei verdrehten Kabeln, auch als "Twisted-Pair"-Kabeln bekannt, bezieht sich auf die Anzahl der Drehungen oder "Twists" pro Längeneinheit im Kabel. Es ist ein wesentlicher Faktor, der die Leistungsfähigkeit der Kabel bestimmt.
  - Eine höhere Schlagzahl hat Auswirkungen auf die elektrischen Eigenschaften des Kabels. Eine höhere Schlagzahl kann dazu beitragen, elektromagnetische Interferenzen (EMI) zu reduzieren, da die enge Verdrehung zu einer besseren Abschirmung der Signale führt. Außerdem kann eine höhere Schlagzahl die mechanische Festigkeit des Kabels verbessern.

  - Bei Twisted Pair Kabel sind die Adern paarweise miteinander verdrillt. Bei dieser Verdrillung ist die Schlagzahl zumeist unterschiedlich groß, wodurch das Übersprechen (ungewollte Signalübertragung zwischen benachbarten Leitungspaaren) zwischen den einzelnen Paaren verringert wird

  - Negative Beeinflussung durch auseinanderdrillen beim Steckerverbindungsbau möglich zu

- **Worin besteht das Problem bei Alien Crosstalk?**
  alien-crosstalk tritt auf wenn mehrere Leitungen parallel laufen

Problem: lässt sich schlecht wegfiltern, weil das Magnetfeld nicht so bekannt ist wie bei verdrillten Adernpaaren. ("Alien" kommt daher, dass diese Art an Crosstalk zwischen verschiedenen Kabeln in einer Gruppe/Bündel passiert und weniger zwischen individuellen Drähten/Leitungen innerhalb eines einzelnen Kabels)
Defacto nicht messbar(da man nicht das andere Signal kennt)

- Mögliche Lösung: Dickere Mäntel/größere Abstände zwischen Pärchen/Kabel
- Übliche Lösung: Schirmung (STP = shielded twisted pair und nicht UTP = unshielded twisted pair)

- **Was versteht man unter Cross Talk? (3 Arten)**
  Über Magnetfelder kann ein Signal von einem verdrillten Adernpaar auf ein anderes Adernpaar Einfluss nehmen. Übersprechen (ungewollte Signalübertragung zwischen benachbarten Leitungspaaren)

  <u>Arten:</u>
  Near-End-Cross-Talk (NEXT)
  An der ersten Steckverbindung nach dem Sender
  Am Ende eines Ethernet-Kabels sind alle Kabel nebeneinander -> Signal kann von einem auf das andere Kabel "überspringen" und wird auf diesem Retour gesendet. Dies ist häufig das Ergebnis elektromagnetischer Interferenzen.

  Far-End-Cross-Talk (FEXT)
  Störung kommt über das Kabel wieder zurück zum Sender wie ein Echo. Weniger dramatisch, weil man ja weiß, was man selbst sagt und das dadurch wegrechnen kann

  Alien-Cross-Talk (AXT)
  Beeinflussung nicht über Aderpaare hinweg, sondern von einem Kabel auf ein anderes. Besonders schlimm, weil man nicht weiß, was man wegfiltern sollte

- **Was ist die Fourier-Analyse und wozu braucht man sie?**
  Ist eine mathematische Methode, mit der ein periodisches Signal in seine Bestandteile zerlegt wird.
  Sie basiert auf dem Konzept, dass jedes periodische Signal als eine Summe von Sinusschwingungen (bzw. Cosinus Schwingungen) unterschiedlicher Frequenzen betrachtet werden kann. Die Fourier-Analyse ermöglicht es, die Amplitude und Phase dieser harmonischen Komponenten zu berechnen, die das ursprüngliche Signal zusammensetzen. Durch die Anwendung der Fourier-Analyse können komplexe Signale in den Frequenzbereich transformiert werden, was es ermöglicht, Informationen über die enthaltenen Frequenzen und ihre Beiträge zur Gesamtsignalform zu gewinnen.

  Anwendung:
  Ermöglicht die Untersuchung und Manipulation von Signalen im Frequenzbereich. Durch die Identifizierung der dominanten Frequenzkomponenten eines Signals können störende Geräusche oder Interferenzen herausgefiltert werden.

Wird vor allem verwendet, um zeitliche Signale in ihre Frequenzanteile zu zerlegen. Aus der Summe dieser Frequenzanteile lässt sich das Signal wieder rekonstruieren.

Signal durch Filter (zB Leitung) -> Signal(untersch. Amplituden) wird (unterschiedlich) gedämpft

- **Unterschiedliche Reichweiten von Richtungsantenne und Stabantenne/Rundstrahlantenne**
  Stabantenne: einige hundert Meter bis zu wenigen Kilometern
  Richtantenne: mehrere Kilometer bis zu einigen Dutzend Kilometern

  Allgemein hängt die Reichweite einer Antenne von verschiedenen Faktoren ab wie Sendeleistung, Umgebungsbedingungen, Hindernisse in der Umgebung.

  Anmerkung:
  Antennen sind gleich gut beim Empfangen und Senden. -> “Bidirektional”

- **Welche Arten von Antennen gibt es und welche Vorteile haben sie?**
  - **Stabantenne**
    senkrechter Stab mit Reflektor
    z.B. Erdoberfläche ist ausreichend als Reflektor,
    rundstrahl Charakteristik

    Quelle: https://en.wikipedia.org/wiki/Antenna_(radio)

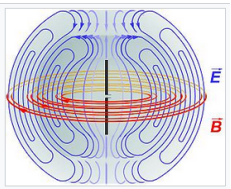
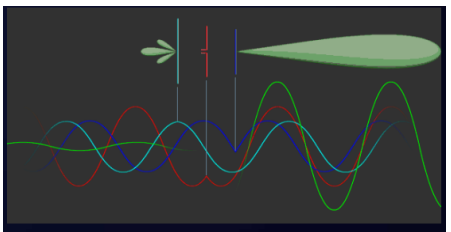
    

    Diagram of the electric fields (***blue***) and magnetic fields (***red***) radiated by a dipole antenna (***black rods***) during transmission.

  - **Richtantenne:** lenkt Signal gezielt in eine Richtung
    90° Gedreht - Direktoren (verstärkt das Signal in eine bestimmte Richtung und trägt zur Bündelung und Fokussierung der elektromagnetischen Energie bei) + Reflektoren
    Richtwirkung einer Antenne: “Hauptkeule”, “Nebenkeulen”, Nullstellen, und Rückwärtskeule
    Störsender kann man ausschalten durch Änderung der Richtung einer Antenne. So weit bewegen, dass der Störsender auf eine Nullstelle trifft (dadurch nicht sichtbar von der Antenne -> keine Störung)

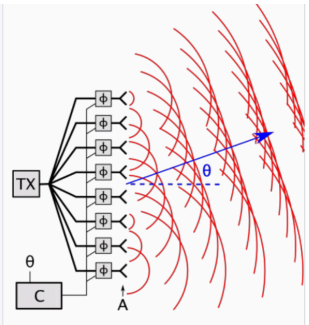
    
    Bild 3: 3–Element-Antenne, Überlagerung der Einzelfelder von Reflektor, Strahler und Direktor

    Quelle: https://www.radartutorial.eu/06.antennas/Yagiantennen.de.html

  - **Antennenarray**

Durch unterschiedliches Ansteuern des Arrays (= Platte mit vielen Antennen n*n) können mehrere Keulen erzeugt werden.

Quelle: https://en.wikipedia.org/wiki/Antenna_array



Animation showing how a phased array works.

- Vertikales/Horizontales Wachstum
  - Vertikal: größere Antennen
  - Horizontal: mehr Antennen (Spannungen addieren sich)

VO4

- **Was beschreibt die EN50173 Norm?**
  - dienstneutrale Verkabelung
    beschreibt, wie eine dienstneutrale Installation von Twisted Pair Verkabelung ausschauen soll. dienstneutral = bin nicht an eine bestimmte Technologie gebunden (TV, Internet, Telefon, … . Dienstneutrale Protokolle: IPv4, Ethernet). Früher musste man für jeden Dienst eine andere Leitung legen.

  - gibt Struktur für den Aufbau der Verkabelung vor:
    Standortverteiler, Gebäudeverteiler, Etagenverteiler, dann zu den Endgeräten Kupferkabeln auf der tertiären Ebenen (= Etagenverteiler), Glasfaserkabeln in den anderen Bereichen

- **Was sind Phased-Array Antennen?**
  viele kleine Antennen die zusammengeschalten sind
  kann durch Ansteuerung d. kleinen Antennen mit der richtigen Phasenlage die Abstrahlrichtung steuern, also wo (in welche Richtung) die Hauptkeule ist und wie breit die Hauptkeule ist.
  Vorteil: kleine Baugröße, elektronisch Nachjustierbar

  Phased-Array: Antennen werden Phasenversetzt angesteuert -> Keule kann ausgerichtet werden

- **Unterschiedliche Qualitätsbezeichnungen: Kategorie vs. Klasse**
  Kategorie = Qualitätsbezeichnung für Kabel
  Bsp: Category 5 Kabel (Cat 5) ist ein twisted pair kabel mit bestimmter Qualität
  6a ist im Moment die übliche Qualität. Allerdings haben alle Stecker, die man dann verwendet, ebenfalls Auswirkungen auf die Qualität.

  Klasse = Qualität der gesamten Datennetz Strecke
  wird mit Buchstaben bezeichnet A, B, C
  es fließt ein:
  - Kabelqualität
  - wie gut die Installation ist (schlecht installiert -> andere Geometrie vom Kabel)
  - Qualität der Stecker
  - …

Kabel dürfen nicht gestückelt werden, da dies eine Störstelle ist, wenn ein LKW drüber fährt, ist das Kabel mehr oder weniger kaputt.

- **Was sind Vorteile und Nachteile von PoE (Power over Ethernet)?**
  Geräte hängen nicht vom Stromnetz ab, sondern bekommen den Strom über das Ethernet. Wird gern für smart buildings, Überwachungskameras, … verwendet. Bis zu 100W/48V Leistung.
  Vorteile:
    - brauche kein extra Stromkabel
    - spare bei Installationskosten

  Nachteil:
    - Funktioniert nur für niedrigere benötigte Stromleistung.
      Ansonsten braucht man möglicherweise dickere Kabeln.
    - Kabel darf nicht zu lange sein damit man genug Spannung hat (~ 100m maximal)
    - zusätzlicher Aufwand beim Einrichten - switch muss dafür konfiguriert werden
    - Gefahren: zu dünnes Kabel, viele Kabel auf einmal -> viel thermischer Widerstand -> Gefahr für Feuer und Schäden

- **Unterschied zwischen Permanent Link und Channel**
  <u>Permanent Link:</u> alles das fix im Gebäude eingebaut wird (Buchse, Kabel dahinter, am anderen Ende wieder eine Buchse)
  Hier wird gemessen, ob die verlegten Kabel gewisse Standards erfüllen.
  <u>Channel</u> = gesamte Strecke also Patchkabel + Permanent Link, Switch, Endgerät
  Wird für den echten Betrieb benötigt

- **Kabelmengen: z.B. Favoritenstraße, Grundfläche, Arbeitsplätze, Etagen, Kabel pro Arbeitsplatz … hochrechnen/abschätzen. Auf ~50km genau(falls möglich)**
  Laut EN50173 Norm hat man:
  Permanent Link bis zu 90m, Patchkabel bis zu 5m auf jeder Seite, insgesamt 100m

  Praxisbeispiel TU Wien Gebäude Gusshausstraße neues ET: 250km Kabel insgesamt verlegt; ca. pro Fenster welches von außen sichtbar ist, 10 Leitungen); Auf einer Kabeltrommel bei der Lieferung hat 1 km Kabel → 250 Kabeltrommeln

  z.B. 50 Fenster pro Geschoß
  5 Stockwerke = 250 Fenster
  Pro Fenster sitzen 1.5 Leute
  Summe: ~500 Leute
  1 Mitarbeiter braucht 2-3 Anschlüsse
  -> 1000 Anschlüsse.
  5 + 40 + 5 = 50m Kabel pro Anschluss
  1000 * 50 = 50 km Kabel
  -> 50 Kabeltrommeln
  -> Man braucht dementsprechend Lagerplatz

- **Unterschied zwischen Pass, Pass* und Fail:**

Wird bei Feldmessgeräten benötigt, bzw. als Ergebnis geliefert: Es werden elektrische Kennwerte von Permanent Links gemessen. Jede Messung ist im Vergleich zu einem Referenzwert. Die Geräte messen auf Promille (10^-3) genau. Schwellenwert(def. durch Referenzwert) liefert outcome:

- pass = gemessene Werte entsprechen den Standards / Normen – liegen in innerhalb der Grenzwerte
- pass* = Grenzbereich, könnte fail oder pass sein. (Ungenauigkeiten in Mess/Referenzelementen, bzw. getestetes Element nur funktionsfähig unter speziellen Bedingungen (z.B. Temperatur zw 20-22 Grad) sonst nicht. "Man steht am Strand und sieht ein Schiff. Was für ein Schiff ist es? -> Wenn es weit weg ist kann man nur vermuten ob es ein Kriegsschiff ist -> pass*"
- fail = Messungen außerhalb der Grenzwerte → mögliche Probleme / Mängel müssen behoben werden

VO5

- **Wie funktioniert MAC Table flooding**

  Schauen, dass die Tabelle im Switch übergeht. Daraufhin schmeißt der Switch die ältesten Einträge weg. Gelingt es d. Tabelle ständig zu überfüllen mit ständig anderen MAC-Adressen, dann kann ich die Tabelle fluten. Wenn 2 andere Stationen Daten austauschen wollen, können die Einträge aus der Tabelle mit den Angriffs-Mac-Adressen überflutet werden -> switch muss das Paket auf allen Ports rausschicken. -> Alle Stationen im Netz bekommen dann alle Pakete zugeschickt -> Man kann die Pakete vom ganzen Netzwerk sniffen.

- **Unterschied zw. single mode und multi mode bei Lichtwellenleitern**

  <u>Lichtwellenleiter allgemein:</u>
  Koaxiales Medium bestehend aus Kernglas und Mantelglas
  Totalreflexion an der Grenze Kernglas/Mantelglas

  <u>single mode phasern</u>
  single mode kann übertragen werden
  Durchmesser Kernglas: 10μm
  Durchmesser Mantelglas: 125μm
  1 μm = 10 ^ -6 m
  Der kleinere Durchmesser ermöglicht eine direkte und geradlinige Lichtübertragung.
  Teurer
  höhere Bandbreite

  <u>multimode phasern</u>
  multi mod: mehrere mode Übertragung möglich
  Kernglas: 50μm
  Mantelglas 125μm

Das Lichtsignal in Multi-Mode-LWL kann aufgrund der unterschiedlichen Ausbreitungsgeschwindigkeiten der Lichtmoden (Energieschwerpunkte nicht in der Mitte des LWL, sondern auf anderen Punkten, da die LW reflektiert an der Außenwand des Kernglases) innerhalb des LWLs auseinandergezogen werden. Dies kann zu einer begrenzten Bandbreite und einer verringerten Signalqualität führen.
Billiger

Single-Mode LWL hat nur 4% der Fläche vom Multimode LWL

- **Entfernungen bei LWL (unterschied Multimode, Singlemode)**
  - Singlemode
    Weniger "Verschmierung" des Signals - bis einige 100 km Distanz einsetzbar. 10 mikrometer Kerndurchmesser - nur 0.6% der Fläche des Mantelglas(125 mikrometer Durchmesser), (siehe Quadratische Skalierung von Single auf Multimode, da Erhöhung des Durchmessers zur quadratischen Erhöhung der Fläche führt)

  - Multimode
    für kürzere Distanzen einsetzbar (ca. 300 - 500m, also im Inneren von Gebäuden). Außendurchmesser 50 mikrometer (16% der Fläche des Mantelglas)

- **Was muss man im Umgang mit Lichtwellenleiter beachten**
  - <u>nie reinschauen</u>
    Bei Lichtwellenleitern niemals hineinschauen, weil die Energiedichte sehr hoch ist aufgrund der kleinen Fläche -> verdampfen der Materie im Auge durch den Laserstrahl im Lichtwellenleiter.

  - <u>Totalreflexion</u>
    LWL arbeiten auf dem Prinzip der Totalreflexion, bei der Licht innerhalb der Faser reflektiert wird. Dafür ist eine korrekte Ausrichtung der Faser wichtig.

  - <u>sehr sauber arbeiten</u>
    Staub in Lichtwellenleitern reflektiert das Licht -> muss bei Lichtwellenleitern sehr staubfrei arbeiten. -> Staub mit Druckluft wegblasen. Nachteil: wegblasen - kühlt ab -> Kondensation

  - <u>maximaler Biegeradius</u>
    Licht breitet sich an sich nur geradlinig aus. Warum bleibt Licht trotzdem im Lichtwellenleiter->Totalreflexion. Licht trifft so flach auf die Grenzfläche zw. den Glasschichten von Kernglas und Mantelglas, das Totalreflexion stattfindet.

  - maximaler Biegeradius
    Problem: die äußere Faser wird stärker gestreckt als die innere.
    Faustregel: 20 Fache Durchmesser des Mantels ist in etwa der Biegeradius

der erlaubt ist.

- <u>Lichtwellenleiter Verlegung - einblasen:</u>
  leere Röhrchen in die Lichtwellenleiter Bündel eingeblasen werden.
  Vorteil: überall im Kabel wird die Kraft über die ganze Strecke aufgebracht.
  Auch zum entfernen aus dem Röhrchen wieder ausblasen, beim ziehen würden sie kaputt gehen.

- <u>Verbindungen:</u>
  Unter Erhitzung aneinander schmelzen -> Ungenaue Verbindung -> Leistungsverlust.

- **Unterschied zwischen lösbaren und nicht lösbaren Glasfaserverbindungen - Lichtwellenleiter Verbindungen**
  <u>nicht lösbare Verbindung:</u>
  zusammenschmelzen durch einen Lichtbogen. Schmilzt das Glas zusammen, wenn die Verbindungen nicht ganz gerade sind, hat man nur einen Teil d. Fläche.
  Wenn d. Glas nicht ganz kreisrund ist sondern leicht elliptisch und die 2 Kabel verdreht -> ebenfalls Verluste
  0.1 - 0.3 Dezibel Dämpfung pro Verbindung
  7 Dezibel Dämpfungsbudget insgesamt

  <u>lösbare Verbindung:</u>
  durch Steckverbindung mit speziellen Steckern
  Stecker sollen möglichst geringe Signaldämpfung besitzen

VO6

- **Wie kann eine Switch-Topologie ausschauen?**
  Switch teilt ein shared media in mehrere Teile.
  Möglichkeiten, mehrere Switches zu verbinden: Kette, Ring, jeder mit jedem:
  - Ketten-Topologie: Switches sind in einer Linie verbunden, wobei jedes Gerät nur zwei Nachbarn hat.
  - Ring-Topologie: Switches sind in einem Kreis verbunden, wodurch jedes Gerät zwei Nachbarn hat und eine Schleife entsteht.
  - Vollständig vernetzte Topologie: Jeder Switch ist mit jedem anderen Switch verbunden.

  Problem: Wenn ein Switch eine Adresse nicht kennt, schickt sie überall hin raus. Und der switch, der es empfängt, kennts wieder nicht und schickts wieder raus. Kann dazu führen, dass Pakete ständig im Kreis geschickt werden, insbesondere bei Broadcasts.
  effektivste Möglichkeit: spanning tree

- **Beschreiben Sie den Spanning-Tree Algorithmus**
  - **bin einziger switch - lerne adressen von paketen**
    neuer switch versucht zu Beginn nachbarn zu finden

Wenn er keinen findet (bekommt keine Antwort in bestimmter Zeit) nimmt er an, er ist allein und fängt an, als Switch zu arbeiten und Adressen von Paketen zu lernen.

- **finde andere switches -> spanning tree erstellen**
  wenn jmd. antwortet - topologieänderung wird erfasst
  -> baue einen neuen Baum auf. Switches unterhalten sich, welche Verbindungen darf ich nicht nutzen, um einen Zyklus zu vermeiden. Wenn ein Switch ausfällt, wird ebenfalls ein neuer Baum aufgebaut. Die Verbindungen, die zuvor vermieden wurden, können dann als Backup-Leitungen verwendet werden.
  Problem: braucht ca. 30 Sekunden um den spanning tree aufzubauen (andere möglichkeit/technologie: rapid spanning tree: geht schneller (2 sekunden))

  Problem:
  Wer wird der root Knoten/core switch vom Baum - sollte nicht ein kleiner switch sein sondern der core switch (ein besonders starker switch) - muss man konfigurieren wer der root knoten sein soll

- **Zeitverhalten beim Weitersenden eines Pakets durch einen Switch**
  - **Store and Forward**
    Beim Store-and-Forward-Verfahren empfängt der Switch das gesamte Paket, speichert es im Pufferspeicher und überprüft seine Integrität. Erst nachdem das vollständige Paket empfangen wurde und keine Fehler festgestellt wurden, wird es weitergeleitet. Dieses Verfahren bietet eine hohe Zuverlässigkeit, da der Switch sicherstellt, dass das gesamte Paket korrekt ist, bevor es weitergeleitet wird. Es kann jedoch zu Verzögerungen führen, da das Paket im Pufferspeicher des Switches zwischengespeichert wird.

  - **Cut Through**
    Beim Cut-Through-Verfahren beginnt der Switch sofort mit dem Weiterleiten des Pakets, sobald die Zieladresse im Paketheader erkannt wird. Dabei werden die Daten bereits weitergeleitet, während das Paket noch empfangen wird. Im Gegensatz zum Store-and-Forward-Verfahren bietet Cut Through eine geringere Latenz. Allerdings bietet es weniger Sicherheit, da der Switch das Paket nicht auf Fehler überprüft. Wenn also ein beschädigtes Paket weitergeleitet wird, kann dies zu Problemen im Netzwerk führen.

  - **Fragment Free**
    Beim Fragment-Free-Verfahren überprüft der Switch die ersten 64 Bytes des Pakets, bevor er es weiterleitet. Da die meisten Kollisions- und Fehlerraten in den ersten Bytes eines Pakets auftreten, dient dieser kurze Überprüfungszeitraum dazu, die Weiterleitung von beschädigten Paketen zu minimieren. Dies bietet eine bessere Sicherheit als Cut Through, ohne die Verzögerungen des vollständigen Store-and-Forward-Verfahrens. Es ist eine Kompromisslösung, die sowohl Latenz als auch Fehlererkennung berücksichtigt.

- **Was ist Flapping?**
  Gibt es bei einem Switch (oder einen Switch-Port), der wiederholt seinen Verbindungsstatus ändert. Dies kann bedeuten, dass der Switch oder Port abwechselnd zwischen "Up" (aktiv) und "Down" (inaktiv) wechselt.

  <u>Problem:</u>
  es muss jedes mal der Spanning tree neu berechnet werden
  Wenn das Flapping erkannt wird, kann es sein, dass der Switch eine Zeit lang automatisch ignoriert wird.
  <u>Ursachen:</u>
  Hardware fehler, software fehler, fehlerhafte konfiguration

- **Was ist link/port aggregation**
  zwei Anschlüsse (Layer 1) werden zu einem logischen Anschluss kombiniert (Layer 2):
  - Gesendet wird immer ein gesamtes Ethernet Paket über eine Leitung
  - Es gibt diverse Algorithmen, um zu entscheiden, wo/wann ein Paket gesendet wird
    - Unterscheidung, wohin ein Paket gesendet werden soll, z.B. anhand der letzten Stelle der MAC Adresse.
  - Höhere Bandbreiten können erreicht werden
  - Dadurch kann Redundanz geschaffen werden (2 Verbindungen räumlich getrennt verlegt)
  - Gegenteil davon: Ein Anschluss für mehrere Verbindungen (VLan)

- **Welche Arten von Wachstum gibt es? (horizontal/vertikal)**
  - **Vertikal:** stärkeren Anschluss (z.B. 10Gb statt 1Gb)
  - **Horizontal:** noch eine Buchse. z.B. (“Port Aggregation”) zwei Anschlüsse (Layer 1) zu einem logischen kombinieren (Layer 2) (siehe vorherige Frage). Dadurch erreicht man theoretisch eine Verdopplung der Bandbreite.

- **CSMA/CD** (Carrier Sense Multiple Access / Collision Detection) **Funktionsweise**
  - CS: “Lauschen”
  - MA: Wenn nichts gehört wird → Kann **jeder** jederzeit zu senden beginnen (also, wichtig: auch mehrere Teilnehmer gleichzeitig).
  - CD: Wenn für mehrere Teilnehmer “nichts zu hören ist” kann es sein, dass diese zur gleichen Zeit senden und es somit zu einer Kollision kommt. → Es ist eine Collision Detection notwendig. Wenn Collision erkannt wird, warten die Teilnehmer eine zufällige Zeit lang → kann dann trotzdem wieder zu einer Kollision kommen, bis zu 8 Mal. In Ethernet-Netzwerken weit verbreitet.
  - Unterschied zu Token Ring: Bei Token Ring hat man Sättigung, hier kann es passieren, dass das System kippt, d.h. keine Übertragung mehr möglich ist.

  - Token Ring:
    Beim Token Ring wird ein spezielles Steuerungspaket, das Token genannt wird, im Netzwerk zirkuliert. Das Token dient als Berechtigung für einen einzelnen Knoten, Daten zu senden. Wenn ein Knoten Daten zu übertragen hat, wartet er, bis er das

Token erhält, fügt seine Daten in das Token ein und gibt es weiter. Dadurch wird kollisionsfreies Senden ermöglicht, da immer nur ein Knoten gleichzeitig das Token besitzt und Daten senden darf
ideal für Netzwerke mit hoher Last & deterministisches Verhalten (spezialisierte Anwendungsbereiche)

VO8

- **Funktionsweise VLAN-Switch**
  VLAN:
  Ein Virtuelles LAN (VLAN) ist ein Netzwerk, das durch Software innerhalb eines Netzwerk-Switches getrennt und definiert wird. Es ermöglicht, dass ein einziger physischer Switch als mehrere separate "virtuelle" Switches fungiert, wobei jeder seine eigene unabhängige LAN-Umgebung bildet.
  VLAN-Switch:
  Ein VLAN-Switch ist ein Switch, der mehrere VLANs verwaltet und den Verkehr zwischen ihnen steuert. Er ermöglicht die Segmentierung eines physischen Netzwerks in virtuelle LANs (VLANs).
  <u>Portbasierte Zuweisung:</u> Der VLAN-Switch weist einzelnen Switch-Ports bestimmte VLANs zu und kann den Datenverkehr zwischen diesen VLANs steuern.
  <u>VLAN-Tagging:</u> Um den Datenverkehr zwischen Switches in verschiedenen VLANs zu ermöglichen, wird eine Tagging-Methode wie IEEE 802.1Q verwendet. Dabei wird jedem Datenpaket ein VLAN-Tag hinzugefügt, das Informationen über das zugehörige VLAN enthält.
  <u>Isolierung und Sicherheit:</u> Durch die Segmentierung des Netzwerks in VLANs kann der VLAN-Switch den Datenverkehr zwischen den VLANs isolieren. Dies bietet zusätzliche Sicherheit, da der Datenverkehr innerhalb eines VLANs von anderen VLANs getrennt bleibt. Der Switch kann auch Sicherheitsrichtlinien implementieren, um den Datenverkehr zwischen VLANs einzuschränken oder zu überwachen.

- **Was bedeutet “virtuell”?**
  Es wird etwas simuliert bzw. imitiert, und innerhalb der Systemgrenzen verhält es sich als wäre es wirklich, aber in Wirklichkeit ist es etwas ganz Anderes.

  In Bezug auf VLANs und insbesondere virtuelle Switches bedeutet dies, dass diese Komponenten so funktionieren und sich so verhalten, als ob sie physische, separate Einheiten wären, obwohl sie tatsächlich durch Software auf einem einzigen Gerät simuliert werden. Diese "Maskerade" ermöglicht es, Netzwerk-Ressourcen effizienter zu nutzen und bietet zusätzliche Flexibilität und Sicherheit, da die "virtuellen" Grenzen innerhalb des Netzwerks so behandelt werden können, als wären sie "echt".

  <u>Vorteile VLAN:</u>
  - Remote-Konfigurierbarkeit:
    VLANs können aus der Ferne konfiguriert und verwaltet werden, was die Netzwerkadministration vereinfacht.

- Einfache Netzwerkreorganisation:
  Durch das Verschieben von Ports zwischen VLANs können Sie das Netzwerk leicht umstrukturieren.
- Erweiterungsfähigkeit:
  VLANs ermöglichen die einfache und kostengünstige Erweiterung des Netzwerks, indem Sie weitere virtuell getrennte Netzwerke einrichten können.

<u>Nachteile VLAN:</u>

- Höhere Kosten:
  VLANs erfordern eine höhere Anfangsinvestition als herkömmliche LANs, da spezielle Switches und zusätzliche Konfiguration benötigt werden.
- Schwierigkeiten beim Austausch:
  Da jeder Switch individuell konfiguriert ist, ist es nicht so einfach, einen ausgefallenen Switch durch einen neuen zu ersetzen. Vor allem, da das gleiche Modell nach ein paar Jahren möglicherweise nicht mehr verfügbar ist und unterschiedliche Firmware möglicherweise eine andere Konfiguration erfordert.

- **Was ist Frequency Hopping?**
  Frequency Hopping ist eine Technik, bei der die Übertragungsfrequenz (in einem drahtlosen Kommunikationssystem) kontinuierlich in einem vorher festgelegten Muster geändert wird. Anstatt auf einer einzigen festen Frequenz zu senden, wechselt das System schnell zwischen einer Reihe von Frequenzen.
  Dient hauptsächlich dazu, die Zuverlässigkeit und Sicherheit der drahtlosen Kommunikation zu verbessern. Wenn bestimmte Frequenzen durch Umwelteinflüsse gestört sind, wird immer nur für kurze Zeit auf diesen Frequenzen gesendet, bevor wieder zur nächsten Frequenz weitergesprungen wird. -> Minimierung von Störungen.

  Zudem erschwert Frequency Hopping das Abhören oder absichtliche Stören der Kommunikation, da ein potenzieller Angreifer das Hopping-Muster kennen müsste, um erfolgreich zu sein. Bei Anwendungen wie WLAN springt das Modem zwischen Frequenzen hin und her, um Störungen auf einer bestimmten Frequenz zu umgehen. Allerdings ist diese Methode besser für Datenübertragungen geeignet, die Unterbrechungen tolerieren können, da kontinuierliche Übertragungen wie Sprachübertragungen durch das Hopping beeinträchtigt werden könnten.

- **VLAN Port-Assignment (3 Möglichkeiten)**
  802.1X Was/Wie/Warum? Authentifizierungsmöglichkeiten bei VLAN

  3 Arten:
  - dynamisch, gibt wiederum mehrere Möglichkeiten:
    - MAC-Adresse
    - Zertifikat (802.1X)
    - username+password
  - statisch
  - Trunk-Port

<u>username + password</u>
funktioniert über den webbrowser
beim ersten webrequest wird nach username/passwort gefragt
Vorteil: geht nur um die Person nicht die Hardware
Nachteil: der computer muss vollständig booten

<u>über MAC Adresse</u>
In diesem Szenario wird das VLAN aufgrund der MAC-Adresse des Geräts zugeordnet. Obwohl dies eine einfache und schnelle Methode ist, hat sie einen wesentlichen Nachteil: die Unsicherheit. Da MAC-Adressen gespoofed werden können, ist dieses System anfällig für Sicherheitsverletzungen.

<u>mittels Zertifikat (802.1X)</u>
Hierbei wird dem Gerät ein Zertifikat ausgestellt, das seine Identität bestätigt. Dieses Zertifikat wird von einer Zertifizierungsstelle (Certification Authority) ausgestellt und erfordert eine Public Key Infrastruktur. Während diese Methode eine höhere Sicherheitsstufe bietet, ist sie auch mit einem erheblichen Arbeitsaufwand verbunden. (Es kann etwa ein Jahr dauern, ein solches System aufzubauen.)

- **Was ist ein Trunk?**
  Ein Layer 1 (Kabel) wird verwendet, um mehrere Layer 2 Verbindungen (VLAN) zu ermöglichen.

  <u>Trunk verbindet mehrere switches</u>
  Mit einem Trunk lassen sich Switches untereinander verbinden. Sie koppeln Netzwerke miteinander und ermöglichen den Aufbau von LANs über mehrere Standorte hinweg. Das lokale Netzwerk ist nicht mehr auf einen einzelnen physikalischen Switch begrenzt, sondern erstreckt sich über mehrere Switches.

  <u>VLAN - Tagging</u>
  Ein Trunk-Port ist ein spezieller Netzwerkport, der so konfiguriert ist, dass er Datenverkehr für mehrere VLANs transportieren kann. Er kennzeichnet die Ethernet-Frames mit zusätzlichen Informationen, um das VLAN zu identifizieren, dem jeder Frame angehört. Dieser Vorgang wird als VLAN-Tagging bezeichnet. Durch die Verwendung von VLAN-Tagging kann der Empfänger die Frames korrekt trennen und an die entsprechenden VLANs weiterleiten.
  (Das gängigste VLAN-Tagging-Protokoll ist IEEE 802.1Q, bei dem jedem Ethernet-Frame ein VLAN-Tag von 4 Bytes hinzugefügt wird. Der Tag enthält Informationen wie die VLAN-ID, die das spezifische VLAN identifiziert, dem der Frame angehört.)

- **Spanning Tree Verhalten bei Störungen**
  (Wenn eine Verbindung beim Spangen-Tree stirbt verwendet man Verbindungen, die man vorher wegen Zyklusbildung vermieden hat.)
  Spanning-Tree-Protokoll (STP):
  STP erkennt Netzwerkänderungen, einschließlich Verbindungsstörungen oder Ausfällen.

- Es startet eine Rekonfiguration des Netzwerks, um zyklenfreie Verbindungen sicherzustellen. Dieser Prozess wird als "Konvergenz" bezeichnet.
- STP kann bestimmte Ports auf den Switches blockieren oder aktivieren, um Netzwerkschleifen zu verhindern.
- Während der Konvergenz kann das Netzwerk instabil sein. Fortschrittlichere Versionen von STP, wie Rapid STP (RSTP), minimieren diese Ausfallzeit.

VO9

- **Welche IP-Netzklassen gibt es? (class A,B,C, Zusatzfrage: direkt auf Bitebene ablesbar)**

  Es gibt drei Hauptklassen von IP-Adressen: Klasse A, Klasse B und Klasse C. Jede dieser Klassen unterscheidet sich in der Anzahl der Bits, die für das Netzwerk und den Host zugewiesen sind:

  - Klasse A: Diese Klasse verwendet 8 Bits für die Netzwerkkennung und 24 Bits für die Hostkennung. Es bietet eine geringe Anzahl von Netzwerken mit vielen Hosts pro Netzwerk.

    Anfang: Erstes Bit immer 0
    Public: 1.0.0.0 bis 127.0.0.0
    Private: 10.0.0.0 bis 10.255.255.255
    Subnet Maske: 255.0.0.0 (8 Bit)
    Anzahl Netzwerke: 126 (128 - Default-Route(0.0.0.0) - Loopback-Adressbereich(127.0.0.0)
    Anzahl Hosts/Netzwerk: 16 777 214
    Broadcastadressen pro Netzwerk X(1 <= X <= 127): X.255.255.255
    Netzwerkadresse: X.0.0.0

  - Klasse B: Verwendet 16 Bits für die Netzwerkkennung und 16 Bits für die Hostkennung. Es bietet eine ausgewogene Anzahl von Netzwerken und Hosts pro Netzwerk.

    Anfang: Erste 2 Bits immer 10
    Public: 128.0.0.0 bis 192.255.0.0
    Private: 172.16.0.0 bis 172.31.255.255
    Subnet Maske: 255.255.0.0
    Anzahl Netzwerke: 16 382
    Anzahl Hosts/Netzwerk: 65 534

  - Klasse C: Diese Klasse verwendet 24 Bits für die Netzwerkkennung und 8 Bits für die Hostkennung. Es bietet eine große Anzahl von Netzwerken, mit einer geringen Anzahl an Hosts.

    Anfang: Erste 3 Bits immer 110
    Public: 192.0.0.0 bis 223.255.255.0
    Private: 192.168.0.0 bis 192.168.255.255
    Subnet Maske: 255.255.255.0
    Anzahl Netzwerke: 2 097 150

Anzahl Hosts/Netzwerk: 254

Die Netzklasse kann direkt auf Bitebene abgelesen werden, indem man das erste Bit (oder die ersten Bits) einer IP-Adresse betrachtet:

- Klasse A: Die ersten 8 Bits (das erste Oktett) beginnen immer mit "0".

- Klasse B: Die ersten 8 Bits beginnen immer mit "10".

- Klasse C: Die ersten 8 Bits beginnen immer mit "110".

- **Warum reichen MAC-Adressen für das Internet nicht aus?**

MAC-Adresse (Media Access Control): ist eine eindeutige Kennung auf Hardwareebene (Layer2). IP-Adressen (Layer 3) ermöglichen die Kommunikation zwischen verschiedenen Netzwerken.
MAC-Adressen sind einzigartig und ein wichtiger Bestandteil von Netzwerken auf Layer 2 des OSI-Modells (wie Ethernet-Netzwerken), aber sie sind nicht ausreichend für das Funktionieren des Internets aus mehreren Gründen:

Keine Unterstützung für Routing
MAC-Adressen ermöglichen nur Punkt-zu-Punkt-Kommunikation innerhalb eines Netzwerks. Sie bieten keine Unterstützung für das Routing von Datenpaketen über mehrere Netzwerke hinweg, was eine grundlegende Anforderung für das Internet ist.

Dynamische Adresszuweisung
IP-Adressen können dynamisch zugewiesen werden, während MAC-Adressen fest in der Hardware verankert sind und sich nicht leicht ändern lassen. IP-Adressen ermöglichen es Geräten, ohne manuelle Konfiguration einem Netzwerk beizutreten oder es zu verlassen.

Hierarchical Routing
IP-Adressen ermöglichen hierarchisches Routing und damit die effiziente Lenkung des Datenverkehrs aufgrund des Netzteils der IP-Adresse.

Netzwerksegmentierung
IP-Adressen ermöglichen die Netzwerksegmentierung, bei der Netzwerke in kleinere Teilnetze unterteilt werden können, um Geräte effektiver zu verwalten und zu organisieren. Jedes Teilnetz kann einen eigenen IP-Adressbereich haben.
MAC-Adressen bieten dieses Maß an Segmentierung nicht.

Skalierbarkeit
IP-Adressen ermöglichen die Skalierbarkeit des Internets, indem sie ein hierarchisches und flexibles Adressierungsschema bereitstellen. Dies ermöglicht die Verbindung von Millionen von Geräten über verschiedene Netze hinweg. MAC-Adressen sind auf die Identifizierung von Geräten innerhalb eines lokalen Netzes beschränkt und nicht für eine globale Skalierbarkeit ausgelegt.

- **Wozu dienen RFC Adressen? (private, nicht geroutete Adressen)**
    - RFC-Adressen, auch bekannt als private IP-Adressen, sind für den Gebrauch in privaten Netzwerken reserviert und können nicht direkt über das Internet geroutet werden. Diese Adressen ermöglichen es, innerhalb eines privaten Netzwerks (wie z.B. einem Heim- oder Unternehmensnetzwerk) Geräte zu adressieren und miteinander kommunizieren zu lassen. Der Einsatz solcher Adressen hilft dabei, den Mangel an verfügbaren öffentlichen IP-Adressen zu lindern. Darüber hinaus bieten sie ein zusätzliches Maß an Sicherheit, da sie von außerhalb des privaten Netzwerks nicht direkt erreichbar sind.

- **Was versteht man unter Maskarading? (Unterschied PAT / NAT)**

Router schreibt lokale IP-Adressen von Clients, die sich hinter dem Router befinden, in public IP-Adressen um.
NAT: 1 lokale IP -> 1 public IP
PAT: 1 lokale IP -> in die einzige vorhandene public IP + nächste freie Port des Routers

<u>NAT (= network address translation):</u>
Router wandelt lokale IP Adresse in public IP Adresse um.
Der Router hat z.B. 5 offizielle Adressen, und im internen Netz gibt's dann 35 Clients, von denen nur 5 gleichzeitig aktiv sind. Die Pakete von einem aktiven Client werden vom Router umgeschrieben und mit einer der 5 offiziellen IP-Adressen weitergeschickt.
Bei ankommenden Paketen schreibt der Router die public IP-Adresse auf die interne IP-Adresse um und schickt das Paket an den lokalen Client.
Wenn ein Client wieder inaktiv ist, wird die IP-Adresse dem nächsten Client zugeschrieben.
Vorteil von NAT: Nur im Layer3 eine Umwandlung, höhere Ebenen (Layer4 - TCP/UDP, Applikationsebene) bleiben unangetastet. NAT wird heute fast gar nicht mehr verwendet.

<u>PAT (= port address translation)</u>
Router hat **eine(1)** Public IP Adresse, die immer verwendet wird.
Router schaut sich die Portnummer im Layer 4 an (TCP/IP paket bzw. UDP paket) und schreibt diese Portnummer um. Schickt Pakete mit der Public IP Adresse und der nächsten freien Portnummer des Routers hinaus. Die Portnummer bleibt dann für den Rest der Kommunikation mit dem lokalen Client konstant.
PAT funktioniert nicht immer (wenn die lokale Port-Adresse des Clients z.b. in der Payload drin ist und diese mit einer Prüfsumme versehen ist -> Bei Portänderung stimmt die Prüfsumme nicht mehr!)

- **IP-Adressberechnung (wichtig siehe VO)**

  Bsp: 192.168.173.216/20

  Die ersten 20 Bit sind die Netzadresse, der Rest ist die Hostadresse.

  IP: 11000000.10101000.10101101.11011000 (192.168.173.216)

  Subnetmaske: 11111111.11111111.11110000.00000000 (255.255.240.0)

Netzwadr.(IP & Maske): 11000000.10101000.10100000.00000000 (192.168.160.0)

Broadadr.(IP | -Maske): 11000000.10101000.10101111.11111111 (192.168.175.255)

VO10

- **Wozu wird ARP verwendet und was ist das?**
  ARP = Address Resolution Protocol
  - Verfahren zur Abbildung einer dynamischen IP-Adresse auf eine permanente (physische) MAC-Adresse in einem LAN
    - Gerät im Netzwerk möchte Daten an eine IP-Adresse senden, aber die MAC-Adresse des Zielgeräts ist nicht bekannt. -> Sendet ARP-Request (Source-IP, Source-MAC, Dest-IP)
    - Alle Geräte im Netzwerk empfangen die Anfrage, aber nur das Gerät mit der entsprechenden IP-Adresse antwortet mit ARP-Reply (Dest-IP=Src-IP[Request], Dest-MAC=Src-MAC[Request], Src-IP[eigene], Src-MAC[eigene])
    - MAC-Adresse wird gecached(ARP-Tabelle im Gerät): (keine ARP-Requests mehr notwendig für diese IP/MAC)
    - Unbedingt notwendig für IP/Ethernet

- **Was ist ARP-Spoofing?** (In welchem Bereich kann das auftreten, was kann man dagegen tun?)
  - Man in the Middle Attack:
    - A schickt ARP mit IP [G] an B
    - B wird von Hacker X daran gehindert.
    - X schickt Antwort zurück und gibt sich als B aus (schickt eigene MAC mit)
    - A glaubt, mit B zu kommunizieren.
    - X bekommt alle Pakete, die nach B gehen sollten.
    - X sendet alle Pakete von A auch an B weiter und alle Pakete von B auch nach A
    - Alles scheint normal, X liest aber alles mit.
    - Potentieller Schaden:
      - Verzögerung der Kommunikation
        - Einzelne Pakete wegwerfen -> viele Retries -> Verzögerung
      - Rohdaten abhören (müssen unverschlüsselt sein, sonst unbrauchbar)
      - Meta-Infos abhören
      - Terminate schicken -> Verbindung unterbrechen
  - Möglich innerhalb eines Switch-Netzes (auch zwischen Endgerät und Router)

- **Skizzieren Sie den Aufruf von www.orf.at** (DNS-Abfragen als Client, Pakete …)
  - Client überprüft DNS-Cache (ist IP-Adresse schon vorhanden?) Wenn nein beginnt die DNS-Auflösung:
    - DNS-Anfrage an die root DNS-Server

            - Antwort: IP-Adressen der DNS-Server für die Top-Level-Domain ".at".
        - DNS-Anfrage an einen ".at" DNS-Server
            - Antwort: IP-Adressen der DNS-Server für die Domain "orf.at" zurück
        - DNS-Anfrage an einen "orf.at" DNS-Server
            - Antwort mit IP von "www.orf.at"
        - Client speichert IP in Cache

- **Was ist ein Name-Server?** (Wie hängen Reverse Name-Server und Name-Server zusammen?)
    - Große verteilte Datenbank
    - DNS-Server sind hierarchisch aufgebaut: Server zuständig für .at, andere für .ac, andere für tuwien etc.
    - DNS-Server kann nicht über einen Namen erreicht werden
        - IP des Servers muss bekannt sein
            - Dynamisch über DHCP
            - Statisch im Gerät eingetragen
    - DNS-Server gibt als Antwort:
        - IP-Adresse vom Ziel
        - IP-Adresse von anderen DNS-Servern, wo weiter gesucht werden soll.
    - DNS-Server kann eine Anfrage an rDNS-Server mit IP-Adresse schicken, um den Hostnamen zurückzubekommen.

- **Was ist ein Reverse Name Server? (Wie hängt er mit Name Server zusammen, worauf muss man achten)**
    - spezieller DNS-Server, der nicht wie ein klassischer DNS-Server Hostname -> IP auflöst sondern IP -> Hostname

    - Einträge im Nameserver und reverse Nameserver müssen zusammenpassen. Besonders wenn sich ein Hostname ändert, muss man sicherstellen, dass beide Server upgedatet werden.

    - Einsatzgebiete:
        - Identifizierung von Spam-Quellen
        - Verifizierung der Echtheit von Emails
        - Sicherheit bei Netzwerkkommunikation
        - Überprüfung und Validierung von IP-Adressen (Herkunft)

- **Was ist DHCP?** (Wie kann man es umgehen, welchen Aufwand hat man damit?)
    - "Dynamic Host Configuration Protocol" ermöglicht die automatische Verteilung von IP-Adressen, Subnetzmasken, Standardgateway, etc. an Geräte(Clients) in einem Netzwerk.
    - Wenn ein Gerät in einem Netzwerk verbunden ist und DHCP aktiviert, sendet es eine DHCP-Anfrage an den DHCP-Server:
        - Der Server antwortet mit DHCP-Antwort (weist Gerät IP und Konfigurationsdetails zu).

- Einfache und effiziente Konfiguration von Netzwerkeinstellungen (v.a. in großen Netzwerken)

- Umgehen mit manueller Konfiguration der IP-Adresse auf den Geräten:
    - IP-Adresse direkt auf jedem Gerät eingestellt
    - Manuelle Konfiguration und Wartung der IP-Adressen -> v.a. in großen Netzwerken sehr zeitaufwändig.
- Gründe dafür:
    - Statische IP-Konfig: bestimmte Geräte erfordern statische IP
    - Sicherheitsaspekte: Sicherheitskritische Umgebung (DHCP als potentielles Risiko) Ohne DHCP können unberechtigte Geräte keine IP-Adressen im Netzwerk erhalten.
    - Netzwerksegmentierung: Teilung eines großen Netzwerks in kleinere. Manuelle Zuweisung, um Segmentierung zu gewährleisten.

VO11

- **Welche Phasen gibt es bei TCP/UDP? (Timeouts, welche Größenordnung von Timeouts)**
  <u>TCP:</u>
  3 phasen: setup, informationsaustausch, Terminierungs phase

  <u>UDP:</u>
  UDP ist ein verbindungsloses Protokoll, bei dem Daten als Datagramme ohne vorherige Einrichtung einer Verbindung übertragen werden.
  Bei UDP weiß man nur durch Timeouts, dass der Sender mit der Übertragung fertig ist.

- **Einsatzszenarien für TCP/UDP**
  <u>UDP:</u>
  Wenn **Geschwindigkeit** wichtig ist und Verlust von Paketen kein Problem darstellt.
  Bsp: z.B. bei Voice-over-IP (VoIP), Videostreaming, Online-Gaming

  <u>TCP</u>
  - **zuverlässige Datenübertragung:** wenn fehlerfreie und vollständige Übertragung der Daten von hoher Bedeutung sind. Bsp: Aufruf von webseiten, emails versenden, datenbank transaktionen

  - **Flusskontrolle und Congestion Control:**
    Nach einer bestimmten Menge an Informationen wird die Übertragung gestoppt und auf ein Acknowledgement von der Gegenseite gewartet. Nachdem die Bestätigung empfangen wurde, wird weiter gesendet. Wenn der Empfänger nicht nachkommt mit empfangen/verarbeiten, dann lässt sich d. Empfänger einfach ein bisschen Zeit mit der Bestätigung -> kann den Sender bremsen, damit ichs verarbeiten kann.

- **Funktion des 3-Way Handshakes**
    - Client sendet SYN an Server.

    - Server sendet SYN-ACK an den Client.
    - Client sendet ACK an Server.

  Dieser Prozess stellt sicher, dass beide Seiten der Verbindung bereit sind und die Sequenznummern synchronisiert sind, um zuverlässigen Datenverkehr zu ermöglichen.

  <u>Sequenznummer</u>
  Die Sequenznummer fungiert als eine Art fortlaufende Nummerierung der TCP-Pakete oder Segmente, die übertragen werden. Die Sequenznummern werden verwendet, um die Reihenfolge der Pakete wiederherzustellen, verlorene Pakete zu erkennen und den Datenfluss zwischen Sender und Empfänger zu steuern.

- **Socket - Aufbau/Anwendung**
  Das Tupel aus ip + port auf der einen und anderen Seite nennt man einen Socket. Der Socket kann auf Betriebsebene weitergegeben werden (z.B. an einen anderen Thread, der nach dem Kommunikationsaufbau die eigentliche Kommunikation abwickelt.)

- SYN-Flood-Attacke
    - Denial-of-Service Attacke, zielt auf dem TCP Protokoll
    - Attacker sendet eine große Anzahl an SYN Paketen an den Server ohne die ACK Antworten zu beantworten
    - Der Server wartet auf die ACK Antworten. Die Verbindung bleibt offen -> Server überlastet und kann keine weiteren Verbindungen von legitimen Benutzer annehmen
    - Abwehrmaßnahmen: Firewalls konfigurieren, spezielle SYN Cookies verwenden, Load Balancer verwenden

- **Standard-Ports (Welchen Port würden Sie verwenden bei Ihrer neuen Applikation?)**

  80: http
  443: https
  25: mail
  110: Pop3
  53: DNS

  <u>Welchen Port würden Sie verwenden?</u>
  Die dynamischen/privaten Ports sind von 49152 bis 65535. Dies ist der Bereich, von wo ich eine Portnummer wählen würde für in-house/lokale Applikationen.

Vorlesungen:

VO2

Thema: Funk
Jedes Gerät, das über Funkwellen kommunizieren will, braucht eine Antenne. Die einfachste Form einer Antenne sind 2 Stäbe.

- Auch ein Stab mit Reflektor (z.B. Erdoberfläche) ist ausreichend
- Direktor (bei Richtantenne): Lenken Signal gezielt in eine Richtung
- Richtwirkung einer Antenne: “Hauptkeule”, “Nebenkeulen”, Nullstellen, und Rückwärtskeule
- Störsender kann man ausschalten durch Änderung der Richtung einer Antenne
    - So weit bewegen, dass der Störsender auf eine Nullstelle trifft (dadurch nicht sichtbar von der Antenne -> keine Störung)
- Vertikales und horizontales Wachstum bei Antennen:
    - Vertikal: größere Antenne (Spiegel)
    - Horizontal: mehrere Antennen (Spiegel)
        - Spannungen addieren sich (Signal von zwei Antennen müssen Phasengekoppelt sein)
    - Antennenarray
        - Durch unterschiedliches Ansteuern des Arrays (= Platte mit vielen Antennen n*n) können mehrere Keulen erzeugt werden

Thema: Kabel (z.B. Ethernet)
Twisted Pair: reduziert Störungen von Magnetfeldern

- Jedes Paar eines Ethernet-Kabels ist verdrillt und hat eine andere Schlagzahl (wie oft verdreht pro Längeneinheit), um sich gegenseitig so gering wie möglich zu stören.

Horizontal: Mehr twisted pairs zur übertragung
Vertikal: Schnellere Frequenz

NEXT: Near End Xross Talk

- Am Ende eines Ethernet-Kabels sind alle Kabel nebeneinander -> Störungsquelle. Das Signal eines Kabels kann auf ein anderes “überspringen” und wird auf diesem retour gesendet.

FEXT: Far End Xross Talk

- Nicht ganz so schlimm: Beim Überkoppeln kommt die Dämpfung der Leitung zugute

Können gut in den Griff bekommen werden, wenn man sauber arbeitet.

Problematisch: Alien Xross Talk

- elektromagnetisches Rauschen, das in signalführenden Kabeln vorkommt, die parallel zu einem oder mehreren anderen Kabeln verlaufen. Der Ausdruck „Alien“ (Fremder) stammt daher, dass diese Art an Crosstalk (Nebensignaleffekt, Übersprechen) zwischen verschiedenen Kabeln in einer Gruppe oder einem Bündel passiert und weniger zwischen zwei individuellen Drähten oder Leitungen innerhalb eines einzelnen Kabels.

VO3

Permanent Link (permanent - alles was nicht aus einem Gebäude bewegt werden kann, z.B. Kabel in Mauer eingebaut)
- Hier wird gemessen, ob die verlegten Kabel gewisse Standards erfüllen.

Channel (alles was man braucht um tatsächlich eine Verbindung aufzubauen, u.a. Patchkabel)
- Wird für den echten Betrieb benötigt
- Switch, Patchkabel, Endgerät

Feldmessgeräte, um elektrische Kennwerte von Permanent Links zu messen.
- Keine Labor Messgeräte
- Jede Messung im Vergleich mit Referenz (Referenz = wie gut ist diese Messskala gemacht worden)
- Auf Promille genau (10^-3) entspricht 10 Bit Auflösung
- Genauigkeit hängt ab von
    - Kurzzeit Veränderung (Temperatur, …)
    - Langzeitveränderung
- Toleranz von etwa 3 db (Faktor 2)
- Schwellwert (def. durch Referenzwert) definiert Outcome (pass/ fail)
    - Schwellbereich: Unsicherheitsbereich (pass*) -> Grenzbereich, könnte pass oder fail sein

Qualitätsbezeichnungen Kabel
- **Kategorie**(Qualität des Produkts vom Hersteller)
    - Einzelkomponente in ihrer Qualität beschrieben
    - Jedes Element (Buchse, Kabel, Stecker) wird durch eine Kategorie in ihrer Qualität beschrieben
- **Klasse**
    - Fertig installierte Strecke wir mit Klasse bezeichnet (Buchstaben)
    - Kombination aus allen Elementen, die eingebaut worden sind, und wie sie eingebaut wurden (Ziehen am Kabel etc.).

ISO 9000 Normenreihe
- Normenreihe, die sich mit Qualitätssicherung und Dokumentation auseinandersetzt

EN50173 Norm
- Beschreiben, wie eine dienstneutrale Installation ausschauen
- Twisted Pair-Kabel können für viele verschiedene Informationsübertragungen verwendet werden (Internet, Fernsehen, Feldbussysteme, …).
- Gibt eine Struktur vor, wie man so ein Kabel aufbauen sollte
    - Primäre Verkabelung (Glas)
        - Standortverteiler (Core Switch)
    - Sekundäre Verkabelung (Glas)
        - Gebäudeverteiler (Distribution Switch)
    - Tertiäre Verkabelung

        - Etagenverteiler (Access Switch) (Kupfer)
            - Twisted Pair Verkabelung zum Arbeitsplatz hin

Dienstneutrales Protokoll (IPV4, IPV6, Ethernet)

Power over Ethernet (PoE)
- 48-58V Strom (60-100W) für das Endgerät (Kameras, wireless access point, Telefonie)
- Vorteil: Endgeräte nicht abhängig von lokaler Stromversorgung
- Kabelstärke wichtig
    - Bei dünnen Kabel Spannungsabfall oder Überhitzung

Insgesamt max. 100m twisted pair Kabel möglich (z.B. 90M permanent, 5m Patch-Kabel auf jeder Seite).

keine Redundanz bei Verkabelung laut Norm → wenn Gebäudeverteiler ausfällt, dann auch alle untergeordneten Etagenverteiler

Dreieck Verbindung
redundante Verbindung zu weiterem Switch in übergeordneten Ebene
man geht aus Norm raus und verletzt strenge Baumstruktur und verwendet Maschenstruktur (führt Redundanz ein) → zB jeden Etagenverteiler mit 2 übergeordneten Ebenen verbinden

Trapez Verbindung auch möglich
- Von Etagenverteiler zu einem anderen Etagenverteiler verbinden
- Nachteil: Anderer Etagenverteiler wird zu einem Transit Switch: Er muss auch andere Daten weiterleiten

VO4

Lichtwellenleiter
- Nicht immer nur gerade verlegt. Möglich durch Totalreflexion:
    - Tritt dann ein, wenn der Eintrittswinkel so klein ist, dass der Ausfallswinkel > 90° zum Lot ist.
    - Medium, das Koaxial ist.
    - .
    - Kleiner Durchmesser -> **Single Mode** Kernglasdurchmesser 10 Mikrometer Mantelglas Durchmesser 125 Mikrometer
        - Einsetzbar bis einige 100km.
    - Großer Durchmesser -> **Multimode** Kernglasdurchmesser 50 Mikrometer, Mantelglasdurchmesser 125 Mikrometer
        - Einsetzbar zwischen 300-500 Meter Entfernung.
        - Für größere Distanzen nicht geeignet.
    - Wieviel Prozent der Fläche des Mantelglasdurchmessers hat die Fläche des Kernglasdurchmessers? ~4%
- Unterseekabel
    - “Unabsichtliche” Beschädigung durch Meerestiere

    - Absichtlich durch Menschen (z.B. unangenehmer Nachbar)
- Nicht in Lichtwellenleiter hineinschauen
    - Hohe Energiedichte -> Verdampfen der Materie im Auge
- Staub in Lichtwellen Anschluss
    - Starke Streuung, wird unbrauchbar
    - Pressluft schlecht, da Anschluss abkühlt -> Wasserdampf kondensiert -> Streuung
- Verbindungen
    - Unter Erhitzung aneinander schmelzen
        - Erhitzung durch Lichtbogen erzeugt.
        - Ungenaue Verbindung -> Leistungsverlust
        - Trotzdem Dämpfung ca. 0.3 db
- Kabel bestehen aus mehreren Fasern, die in einem gemeinsamen Kabelmantel zusammengefasst sind.
    - Problem beim Biegen. Biegeradius heikel
        - Daumenregel: 20 Fache Durchmesser des Kabelmantels ist der erlaubte Biegeradius
- Verlegung mit leeren Röhrchen: Mehrere Lichtwellenleiter werden “eingeblasen”.
    - Durch raue Oberfläche mit Luft “eingeblasen”.
    - Vorteil: Über die gesamte Länge wird die Vorwärtsschubkraft aufgewendet.
- Bandbreiten:
    - Gigabit/s bis 100 Gigabit/s
- Mehr Bandbreite benötigt:
    - Mit unterschiedlichen Farben hineinleuchten
    - Aufteilung mittels Prisma am Ende
    - Über eine Faser mehrere Kanäle übertragen
    - Bidirektionale Übertragung über selbe Faser dadurch möglich
- Eingesetzt
    - Zwischen Standortverteiler - Gebäudeverteiler - Etagenverteiler
- Beispiel:
    - Gebäudeverteiler mit Router und Switche
    - Datennetz nutzen um Management darauf zuzugreifen
    - Alternative: Parallel Netz um Management zu betreiben
        - Vorteil: Auch verfügbar, wenn Datennetz nicht verfügbar ist

Ethernet

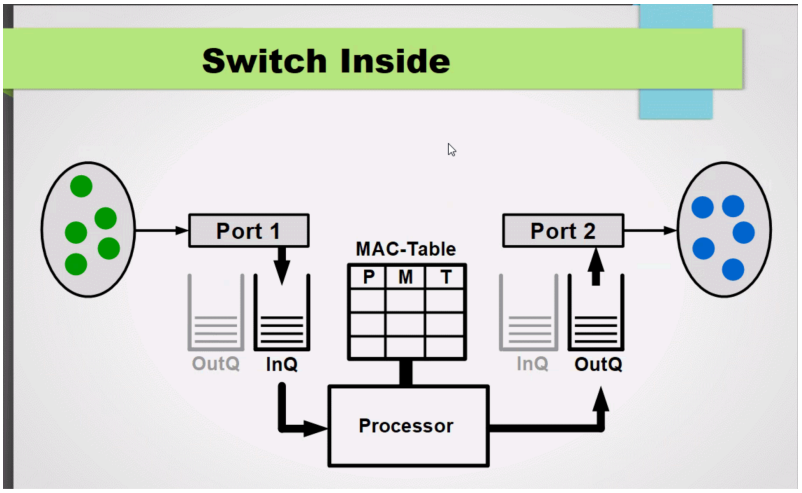
- Man braucht immer ein Medium, in dem sich die EM-Welle ausbreitet
- Ursprünglich: Koaxialkabel, mit Vampirklemmen drangehängt. Auf 1 Kabel viele Geräte angeschlossen -> “Shared Media”
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
    - Asynchrone Übertragung (Kein zentraler Takt, Zeitverschiebungen)
    - 1. Lauschen, ob andere Station gehört werden kann
        - Wenn nichts gehört wird -> Medium frei
        - Ich kann mit meiner Aussendung beginnen
        - Kann passieren, dass mehrere Sender senden
        - Kommt zu einer Kollision, die beide mitbekommen müssen
        - Überlagerung von Aussendungen, nicht detektierbar

        - Zeit: Kollision - Recovery ist verloren (reduziert gesamt verfügbare Bandbreite)
    - Bei Überlast kommt es zu einem Breakdown
- Längenbegrenzung / Laufzeiten
    - Erst mit 2x Laufzeit bekommt der Sender mit, dass es eine Kollision gegeben hat
    - Mindest-Sendedauer muss gegeben sein, die der Dauer des Hin- und Rücksendens entspricht.
- Heutige Netze
    - Punkt-zu-Punkt Verbindung
    - “Trennwände” einführen -> 2(oder mehr) Teile, die die volle Bandbreite nutzen können
    - Switch
        - Empfängt Daten. Überprüft wo es hingehört. Wenn es auf die “andere Seite” gehört, schickt er es dorthin.
        - Funktionsweise:
            - Kriterien eines Shared Media: Adressierung, Zugriffsmethode, Selbstbeschränkung
            - OSI Layer 2: MAC-Adresse (6 Byte, durch Hersteller der Hardware definiert, kann auch von Software überschrieben werden)
            - MAC Zieladresse (Wer ist damit gemeint, wo soll die Nachricht hingehen), MAC-Absenderadresse (Meine Nachricht kann beantwortet werden)
            - Absender MAC-Adresse in die Tabelle schreiben. Zieladresse in der Tabelle suchen. Empfangenes Paket wird an Zielport hinausgeschickt.
            - Switch ermittelt Zielport durch Metadaten, die in empfangenen Paketen enthalten sind.
            - Wenn die gesendete Nachricht auf dem gleichen Port wie die Zieladresse adressiert ist, kann der Switch die Nachricht verwerfen, da sie eh durch das Shared Media vom Empfänger empfangen werden kann.
            - Nicht zuordenbares Paket muss an alle Ports (Ausnahme der Port, wo es empfangen wurde) senden.
        - Angriffsmethode(Mac Table flodding): Tabelle vollfüllen
            - Dadurch wird der älteste Einträge weggeschmissen
            - Neue Einträge werden stattdessen eingetragen
            - Wenn Tabelle permanent überfüllt wird mit Nonsenseadressen, wird die Tabelle überflutet. Wenn 2 andere Stationen Daten austauschen wollen, können die Einträge aus der Tabelle mit den Angriffs-Mac-Adressen überflutet werden. Dadurch muss der Switch immer alle eingehende Nachrichten auf alle Ports rausschicken. Dadurch kann der Angreifer mithören, da die Pakete an alle Ports geschickt werden.

VO5

Ergänzung Switch

- Entscheidung des Switch
  - Broadcast (für alle, daher an alle)
  - Ignore (schon erledigt)
  - Forward (weiterleiten zum Ziel)
  - Flooding (überall, irgendwo muss er ja sein)
  - Discard (korrupt, daher verwerfen)
- Zeitverhalten
  - Store and Forward (vollständig speichern, prüfen und ggf. weiterschicken)
  - Cut Through (ggf. noch während des Empfangens bereits weiterschicken)
  - Fragment Free (erst dann ggf. weiterschicken, wenn keine Kollision war)



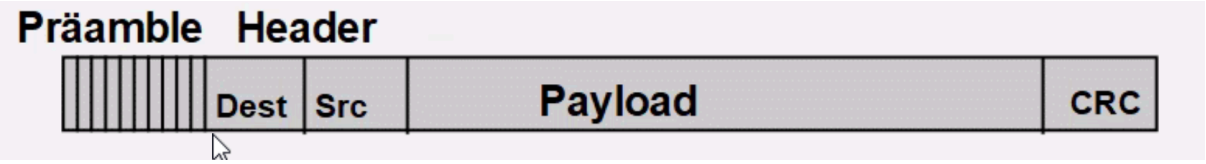
P… Port wo Paket hereinkommt
M … MAC-Adresse vom Absender
T … Time

MAC-Table muss nicht dynamisch sein, kann auch statisch eingefroren werden (advanced Feature, meist nicht möglich)

- Anmerkung: Prozessor stellt Pakete unverändert in die Outport-Queue.
- Problem: Queue kann voll werden (Queue ist begrenzt)
  - Input-Queue kann übergehen: Mehr Pakete kommen rein, als der Prozessor verarbeiten kann.
    - “Full wire speed”: Egal wie viele pakete reinkommen, der Prozessor und Speicher ist ausreichend dimensioniert, dass alles verarbeitet werden kann
  - Output-Queue kann übergehen: Viele Datenströme auf verschiedenen Ports kommen herein (Pakete werden weggeschmissen)
    - Selbst ein “full wire speed”-switch kann das nicht garantieren
- MAC-Table
  - Größe: 1000-4000 Einträge (nicht dynamisch erweiterbar)
  - Siehe MAC-Table flooding (VO4)
- Rollen eines Switches
  - Primäre Rolle: Pakete empfangen und ggf. weiterleiten

- Management Rolle: Anfragen und Aufträge des Managers bearbeiten
    - braucht CPU-Leistung (auch Speicher etc.)
    - Variante 1:
        - Alle Ressourcen einsetzen, um die primäre Rolle zu erfüllen.
        - Zweite CPU hinzufügen, der die Management Rolle erfüllt.
    - Variante 2:
        - Overhooking: Verkaufe mehr als ich habe, in der Annahme, dass eh nicht alle gleichzeitig etwas wollen.
        - Annahme: Manager wird sehr selten fragen, wenn er bei Hochlast fragt, muss er später noch mal fragen.
    - Frage, die man sich stellen muss: Welche Rolle soll Priorität haben?
        - Wenn die primäre Rolle Priorität hat, kann es sein, dass Management-Anfragen verworfen werden (z.B. zur Fehlersuche).

Ergänzung Ethernet:
Ethernet-Paket:



- Präambel:
    - Serie aus 101010 etc, damit Empfänger Zeit zwischen Bits berechnen kann (Phasenangleich)

VO6

Spanning Tree algorithmus / Spanning Tree:

- Wenn ein Switch booted -> Lernmodus
- Versucht, Nachbarn zu finden, die auch Switches sind
    - Wenn er keinen findet (nach Timeout): Ich bin alleine -> ab dann wird der typische Switch Mechanismus gestartet
    - Wenn er wen findet -> Topologieänderung
        - Ein neuer Baum wird aufgebaut. Es wird festgestellt, welche Verbindungen nicht genutzt werden dürfen, um einen Zyklus zu verhindern.
        - Vorteil: Wenn eine Verbindung ausfällt, wird ein neuer Spanning Tree aufgebaut (Dauert ca. 30 Sek., mit z.B. einer Verbindung, die vorher nicht genutzt werden durfte). Nennt man “selbstheilende Funktion”
        - Probleme: z.B. Gerät, das über das Netzwerk das Bootimage holt: Dadurch, dass es 30 Sek. dauert, bis der Switch normal arbeitet, fällt das Gerät in einen Timeout und kann nicht booten.
        - Wichtig: Definieren, wer der Root-Switch ist (damit nicht schwacher Switch die größte Last tragen muss)

3 Layer von Switches:

- Core Switch
- Distribution Switch

- Access Switch

Horizontales vs. Vertikales Wachstum:

- Vertikal: stärkeren Anschluss (z.B. 10Gb statt 1Gb)
- Horizontal: z.B. (“Port Aggregation”) zwei Anschlüsse (Layer 1) zu einem logischen kombinieren (Layer 2) (gesendet wird immer ein gesamtes Ethernet Paket über eine Leitung. Gibt diverse Algorithmen, um zu entscheiden, wo/wann ein Paket gesendet wird.)
    - Dadurch kann auch Redundanz geschafft werden, indem die zwei Verbindungen räumlich getrennt verlegt werden. Wenn eine Verbindung ausfällt, kann der Traffic auf die andere übertragen werden.
    - Gegenteil: Ein Anschluss für mehrere Verbindungen (für virtuelles LAN)

VO7

Virtuelle LANs

- Virtuell -> “echt erscheinend”, Maskerade (virtuelle grenzen verhalten sich wie in echt, das innere anders)
- VLAN Switch -> Eigentlich eine Box mit vielen Komponenten, auf denen eine Software läuft, die einen virtuellen Switch darstellt. Ein Gerät kann mehrere Switches simulieren, da es sich nur um Software Prozesse handelt, nicht um “echte” Switches.
- Systemspezifikation: Abweichungen davon führen oft zu Fehlern
- Statische Zuordnung:
    - Physikalische Ports am VLAN Switch werden verschiedenen virtuellen Switches zugeordnet.
    - Fixe Zuordnung auf unterschiedliche virtuelle Switche.
    - Zwei Geräte die an unterschiedlichen Ports hängen können nicht auf den anderen zugreifen -> können auch nicht gehackt werden
    - Domänen können geschaffen werden: z.B. Entwicklung, Finanzen, Geschäftsführung. Die Domänen können nicht auf die anderen Domänen zugreifen (Security)
    - Bei Broadcast-Paket schickt ein virtueller Switch das Paket an alle (außer sich selbst) die an ihn hängen (an diesem virtuellen Switch). Die anderen virtuellen Switches bekommen davon nichts mit. -> Layer 2 Broadcast wird durch virtuelle Switches beschränkt.
    - VLAN über mehrere “Kisten” auch möglich
        - Rein durch Software möglich.
        - Praktische Anwendung: TU, Räumlichkeiten eines Instituts verteilt -> VLAN für das Institut mit einem VLAN für einen anderen Raum verbinden. -> hängen dann im selben VLAN
- Problem: mehrere VLAN Switches verbinden:
    - Trunk: Eine Verbindung mit genug Bandbreite zwischen zwei VLAN S. Tag zu Paket hinzufügen, das definiert, zu welchem virtuellen Switch das Paket gehört (z.B. dieses Paket gehört zu VLAN_1) (Spielt sich im Layer 2 ab)
- Frequency Hopping
    - WLAN Modem springt zwischen Frequenzen hin und her, falls es auf einer Frequenz Störungen gibt.

    - gut bei datenübertragung die nicht ununterbrochen sein muss, sprachübertragung ist beispielsweise problematisch
- Default VLAN: Wenn keine Zuweisung zu einem bestimmten VLAN erfolgt, hängt der Port am default VLAN
- Problem: wenn VLAN Switch ausgetauscht werden muss: Wie konfiguriere ich den neuen Switch?
    - VLANs zuerst bei allen Switches definieren, dann erst physische Ports zuordnen.
    - neue Switches können diese VLANs dann einfach übernehmen.
    - System von Cisco:
        - Neuen Switch hinzufügen mit neuer Konfiguration inkl Config Nr., alle Switches fragen dann untereinander wer die höchste Config Nr. hat und konfigurieren sich untereinander
        - Vorteil: Änderung nur an einer Stelle notwendig.
        - Problem: Switch wird zuerst mit Test-VLANs getestet. Wenn diese Test VLANs (aus Versehen) eine hohe Versionsnummer haben, kann es sein, dass alle anderen Switches diese Test-VLANs übernehmen und die richtigen VLANs löschen (Portzuweisung ist weg! Alle Ports sind dazwischen auf den Default VLAN zugewiesen geworden, da die anderen VLANs gelöscht wurden. Die $f$ordnung kann nicht durch eine Verteilung einer neuen Konfiguration erfolgen!). → Backup wird gebraucht.

- Dynamische Zuordnung:
  Switch fragt nach Identität vom angeschlossenen Gerät, ordnet aufgrund dessen dem Port ein VLAN zu.
    - Authentifizierung durch Username + Passwort (automatisiert oder manuell über zB Webbrowser)
        - Vorteil:
            - keine manuelle Konfiguration notwendig.
            - Zugang ist nicht auf die Hardware sondern auf die eingeloggte Person zugeordnet
        - Nachteil:
            - Man braucht eine Person, um sich einzuloggen.
            - Der Switch braucht mehr Rechenleistung
            - Gerät muss schon booten können (kann bei manchen Geräten nicht der Fall sein)
    - Authentifizierung über die MAC-Adresse:
        - Zugang ist auf die Hardware zugeordnet (unsicherste Variante)
    - Authentifizierung über Zertifikate:
        - Jedes Gerät wird ein Zertifikat gegeben, das anschließend abgefragt wird.
        - Man brauch Certification Authorities und Public Key Infrastructure (PKI)
        - Wird für Sicherheitskritische Bereiche verwendet.
        - Sehr großer Aufwand

VO8

Layer 3

- Warum IP Adressen? Man könnte ja alles mit MAC Adressen verbinden (Punkt zu Punkt). Internet = netz zwischen netzen, internet verbindet netze,
  wenn ich mehrere Layer 2 Netze verbinden möchte, passiert das auf dem 3. Layer (Network)
- Network Layer -> Verbindung zwischen mehreren Layer 2 Netzwerken
- Geräte in Layer 3: Router (nicht layer 3 switch als bezeichnung verwenden)
  - Router sieht sich nur Layer 3 Adresse an (IP Adressen). Kümmert sich nicht um Layer 2.
  - Router hat Layer 2 u 1 sehr wohl implementiert damit Payload zu Layer 3 hinaufkommt, switcht aber nicht
  - Brouter: bridge router kann auf layer 2 switchen und auf layer 3 routen
  - Bridge und Switch agieren auf Layer 2, Router auf 3.
- IP Protokoll
  - neben IP mehrere Protokolle auf Layer 3 (TechNet?), IPv4 und IPv6 sind über geblieben
  - 32 bit > werden in 8er gruppen geteilt, punkt ist nur für human readability (nicht Teil der eigentlichen adresse)
    - Wertebereich 0 - ~4.3 Mrd mögliche Adressen
    - Kann man auch als Integer darstellen
    - Verschiedene Klassen: siehe auch https://www.meridianoutpost.com/resources/articles/IP-classes.php
      - Class A (8 Bit Netz, 24 Bit Host)
      - Class B (16 Bit Netz, 16 Bit Host)
      - Class C (24 Bit Netz, 8 Bit Host)
  - Anfängliche Routingtabellen 64k Einträge
    - relativ schnell voll
  - Lösung: Class C Netze wurden zusammengefasst um mehr Einträge erreichen zu können (192.168.0.0 und 192.168.1.0, Netzmaske um eins nach links verschieben)
  - Router Lebensdauer 5 Jahr (10 Industrie): in 5 Jahren gibts so viele neue Geräte mit mehr Speicher in Umlauf, dass sich Problem von selbst löst
  - Subnetmaske z.B. 4 Bit -> 2^n - 2 Adressen können verwendet werden. Wenn man mehr Geräte verwenden will -> Subnetmaske verschieben: 5 Bit -> Viele mögliche Adressen ungenutzt
  - für Punkt zu Punkt verbindung zwischen 2 Router brauche ich 4 Adressen (2 kann ich nicht nutzen)
  - TU-Wien hat 2 Class B Netze: 128.130… 128.131…
- Was, wenn IP-Adressen ausgehen?
- Unterscheidung in:
  - Server (bietet an, wartet, dass ein Client etwas verlangt, passiv)
  - Client (bietet kein Service an, nutzt Service, Initiative geht immer vom Client aus, aktiv) -> bekommen 192(oder 172?) Adressen, da sie eigentlich keine eigene Adresse benötigen, da sie per Definition nicht ansprechbar sein müssen. 192(oder 172?) Adressen kommen im Internet nicht vor.
  - https://de.wikipedia.org/wiki/Private_IP-Adresse

        - Private Address Ranges (RFC Adressen)
            - Class A: 10.0.0.0 to 10.255.255.255
            - Class B: 172.16.0.0 to 172.31.255.255
            - Class C: 192.168.0.0 to 192.168.255.255
- Masquerading:
    - Damit private Adressen im Internet verwendet werden können
    - Unterscheidung:
        - PAT (Port Address Translation)
            - Wandelt interne Adresse in offizielle Adresse um
            - Hat 1 IP Adresse nach außen
            - Wandelt TCP/UDP-Pakete um (bis Layer 4) und schreibt Portnummer um: Welche Portnummer auf der externen Seite wurde noch nicht benutzt -> verwendet diese
            - PAT funktioniert nicht wenn Portnummer auch in Payloads vorkommt -> Gerät müsste dann auch in Payload schauen und dort Portnummer umschreiben -> kann es nicht.
        - NAT (Network Address Translation)
            - Gerät hat mehrere IP Adressen (zB 5) und verwaltet viele Clients (zB 35).
            - Nimmt an, dass nicht alle gleichzeitig aktiv sind.
            - Gibt unterschiedlichen clients unterschiedliche Adressen.
            - Wenn ein Client wieder inaktiv ist, wird IP Adresse dem nächsten Client zugeschrieben.
            - siehe auch https://mcse.körbel.at/links/grundlagen/netzwerk/nat.htm
    - Transformiert zu Paketen, die über das Internet verwendet werden können
- Im Layer 3 gibt es auch 2 verbotene Adressen (nicht nutzbar für Endgeräte): Broadcast (Hostteil alles 1, Netzteil unverändert) und Netzwerk (Hostteil alles 0 = “Netzadresse”)
- Wir sollen mit IPv4 adressen rechnen können für Prüfung (boolesche Algebra)
    - Netzwerkadresse = IP (logisches UND) Netzmaske
    - Broadcastadresse = IP (logisches ODER) NOT(Netzmaske)
- Für Prüfung: nur mit Papier & Stift! → **Fünfer** wenn man das nicht kann :)

Rechenbeispiel:
Angabe: 192.168.173.216/20 → Erste 20 Bit sind Netz, Rest ist Host.

```
IP Adresse:    11000000.10101000.10101101.11011000
Subnetmaske: 11111111.11111111.11110000.00000000 = 255.255.240.0
Netwerkadr.:   11000000.10101000.10100000.00000000 = 192.168.160.0
Broadcast.:    11000000.10101000.10101111.11111111 = 192.168.175.255
```

(https://www.browserling.com/tools/ip-to-bin, https://www.browserling.com/tools/bin-to-ip)

- Wenn ein Paket an die Netzwerkadresse gesendet wird, kann eine Antwort kommen, muss aber nicht.

DAS AUF JEDEN FALL ÜBEN! (Kann sonst sein dass man **negativ** ist lol)

9 Möglichkeiten wie ein (Grenz-)Byte in einer Subnetmaske ausschauen kann
Wie lauten diese 9 Varianten dezimal?
10000000 = 128
11000000 = 192
11100000 = 224
11110000 = 240
11111000 = 248
11111100 = 252
11111110 = 254
11111111 = 255
(note: alle gerade außer 255, sprich alles 1, also wenn bei der subnetzmaske am 3. byte eine ungerade zahl steht die ungleich 255 ist, dann stimmt hier was nicht → reinleger den er geben könnt)

- Routing Beispiel: Layer 2 und Layer 3, Client sendet Paket an Router, Router (über ARP-Requests (für MAC-Adressen)) an Server (hierzu könnten wir nächste Stunde das Beispiel nochmal durchgehen)
    - Dass ein Router das Paket verarbeitete, weiß er aufgrund der mitgelieferten MAC Adresse, dass diese mitgeliefert werden kann, davor wurde auf diesen Router ein ARP Request gemacht, die MAC Adresse erhalten und dem Paket beigefügt.

VO9

Address Resolution Protocol (ARP): ist ein Verfahren zur Abbildung einer dynamischen Internet-Protokoll-Adresse (IP-Adresse) auf eine permanente physische Maschinenadresse (MAC-Adresse) in einem lokalen Netzwerk (LAN)

- Request: Source IP, Source MAC, Destination IP
- Destination MAC wird gesucht (durch Broadcast)
- Antwortpaket: Destination IP=Source IP vom Request, Destination MAC = MAC vom Request, Source IP = eigene IP, Source MAC = eigene MAC
- Antwort wird in den Cache des Senders geschrieben.
- Layer 2 und 3 sind hier miteinander verwoben
- Unbedingt notwendig für IP/Ethernet

ARP Spoofing (Man in the Middle attack):

- Station A schickt ARP request mit IP an Station B
- Station B wird vom Hacker X daran gehindert.
- Hacker X schickt Antwort zurück und gibt sich als B aus (und schickt eigene MAC-Adresse mit)
- Station A glaubt nun, mit Station B zu kommunizieren, es ist aber X.
- X bekommt nun alle Pakete die nach B geschickt werden sollten
- Er sendet alle Pakete auch an B weiter und umgekehrt.
- Es scheint alles normal, nur liest Hacker X alles mit.
- Hacker X könnte:
    - Kommunikation verzögern

        - Einzelne Pakete verwerfen -> Retries -> große Verzögerungen
        - Rohdaten abhören (wenn verschlüsselt dann nicht brauchbar (müssten entschlüsselt werden)
        - Meta-Informationen abhören
        - Ein Terminate schicken -> Verbindung unterbrechen
    - Geht nur innerhalb eines Switch-Netzes (nicht über Router)
        - Aber auch zwischen Endgerät und Router möglich

IP-Adressen sind abhängig vom Netz (müssen aber innerhalb dieses Netzes eindeutig sein)
Verwaltung solcher Adressen:
- Zentrale Verwaltung
- Automatismus (DHCP)

IP-Adresse topologisch abhängig (je nachdem wo ich mich befinde bekomme ich eine IP-Adresse)
Internet-Namen sind hierarchisch organisiert.
- tuwien.ac.at
- .at -> Österreich (topologisch festgelegt, geographische Grenzen)
    - Ist aber nicht sichergestellt, dass alles was mit .at endet sich in Österreich befindet
    - Hat dadurch nicht wirklich eine Aussagekraft
- 3-Buchstabige Domains .com, .gov, .net sind besonders:
    - Von den USA ausgehend:
        - .com -> commercial
        - .gov -> government
        - .net -> Rest
- Zusätzliche Namen dazugekommen mit mehr als 3 Zeichen:
    - .xxx
    - .info

Auflösungen passieren über DNS(-Server):
- Sehr große verteilte Datenbank
    - hierarchisch aufgebaut: Ein Server zuständig für .at, einer für .ac, einer für tuwien, etc.
    - DNS-Server kann nicht über einen Namen erreicht werden
    - Wenn man einen DNS-Server betreibt, müssen die Geräte so konfiguriert werden, dass die IP-Adresse des Servers bekannt ist.
        - Dynamisch über DHCP
        - Statisch in das Gerät eingetragen
    - DNS-Server gibt entweder
        - Antwort mit IP-Adresse
        - Hinweis wo weiter gesucht werden soll
- Caching-System:
    - Änderung bei einem DNS-Server
    - Erst bei Nachfrage wird die neue Antwort gegeben (Bei Änderung des Namens kann es eine Zeit lang dauern, bis alle höherrangigen DNS-Server ihren Cache aktualisiert haben.
    - Lösung: Beide Namen aktiv halten für ein paar Tage, bis umgestellt wurde

- A-Records auf einem DNS-Server und Pointer-Records auf einem anderen DNS-Server müssen konsistent sein
- Statische Konfiguration:
    - Immer noch erreichbar auch wenn DHCP-Server nicht mehr erreichbar ist
- Dynamische Konfiguration:
    - Gute Flexibilität

VO10

Layer 4: Transportschicht

- UDP (User Datagram Protocol)
    - wartet nicht auf Antwort/Bestätigung
    - Wenn ein Paket nicht vollständig ankommen, muss auf dies auf der Applikationsebene gemanaged werden
    - Vorteil:
        - Kurze Zeit
        - Kein setup
    - Nachteil:
        - Nicht kontrolliert
    - Wie kommt man drauf, dass der Gesprächspartner nicht mehr zuhört?
        - Timeout
    - Usecase:
        - Kleine IoT devices mit remote Boot-Image
            - Wenn File mit Checksumme übertragen wird und checksumme falsch ist, fordert das device die Pakete wieder an
- TCP (Transmission Control Protocol)
    - Führt zuerst ein Setup durch, um sicherzustellen dass sich 2 Parteien gegenseitig hören:
        - Danach kommt erst die eigentliche Information
        - Schlussendlich kommt eine Terminierungsphase
        - 3 Way Handshake bei Verbindungsaufbau und Terminierung
    - Flusskontrolle:
        - Zwischendurch unterbrochen und auf Bestätigung warten
        - Wenn die Bestätigung länger dauert, kann man so den Sendenden bremsen
        - Nachteil: Laufzeit des Signals für Hin-/Zurück muss immer abgewartet werden.
            - Wenn Taktrate 10^9 und signal braucht 1ms (10^-3), dann muss der Rechner 10^6 (1mio) Takte warten.
    - 3-way-Handshake Probleme:
        - Jemand klopft bei Tür an -> Der im Raum sagt “herein”
        - Jemand geht weiter und klopft bei der nächsten Tür an
        - Die Personen in den Räumen werden unterbrochen, warten auf eine Antwort
            - Wie lange warten?

            - Ressourcen werden währenddessen gebunden (File-descriptors)
    - Usecase:
        - Wenn Austausch kritischer/heikler ist
- Auf zwei IP-Adressen mehrere Services angeboten:
    - Müssen unterschieden werden mit “Ports”
    - Erwartete Ports (nicht zwingend genau diese Ports für diese Services)
        - 53 - DNS
        - 80 - Http
        - 443 Https
        - 5000 - ?
        - 6000 - ?
        - 8080 - ?
    - Tupel aus IP-Port vom Sender und IP-Port vom Empfänger ist ein Socket
        - Socket kann weitergegeben werden an ein Kind, das eine Anfrage bearbeitet (Wenn viele Anfragen kommen, die (parallel) bearbeitet werden sollen)
        - Möglichkeiten:
            - Neuen Prozess erstellen mit fork (teuer)
                - Wichtig: mitzählen, wie viele Prozesse laufen, terminieren wenn Prozess fertig. Vor Termination: von Liste aller Prozesse austragen.
            - Gleich zu Beginn mehrere Prozesse erstellen, die schlafen
                - Wenn eine Anfrage kommt, weckt der Hauptprozess ein Kind auf und übergibt ihm den Socket